Tatouage d'images numériques par paquets d'ondelettes

Anne Manoury

Ecole Centrale de Nantes *Université de Nantes*

ÉCOLE DOCTORALE

SCIENCES ET TECHNOLOGIES
DE L'INFORMATION ET DES MATERIAUX

Année 2001

Thèse de DOCTORAT

Diplôme délivré conjointement par L'École Centrale de Nantes et l'Université de Nantes

Spécialité : AUTOMATIQUE ET INFORMATIQUE APPLIQUEE

Présentée et soutenue publiquement par :

ANNE- MANOURY

le 21 Décembre 2001
à l'Ecole Centrale de Nantes

TATOUAGE D'IMAGES NUMERIQUES PAR PAQUETS D'ONDELETTES

Rapporteurs :	Jean-Marc CHASSERY	Directeur de Recherche CNRS ENSIEG Grenoble
	Benoît MACQ	Professeur UCL Louvain-la-neuve
Examinateurs :	Henri MAITRE	Professeur ENST Paris
	Jacques LEVY-VEHEL	Directeur de Recherche INRIA Nantes
	Marie-Françoise LUCAS	Maître de Conférences ECN Nantes
	Philippe NGUYEN	Ingénieur de Recherche Thalès Communication Paris

Directeur de thèse : Jacques LEVY-VEHEL
Laboratoire : Institut de Recherche en Communication et Cybernétique de Nantes N° ED 0366-056
1, rue de la Noë , BP 92101, 44321 Nantes Cedex 03

Tatouage d'images numériques par paquets d'ondelettes

Anne Manoury

Remerciements

Ces trois années de thèse ont été riches en moments de toutes sortes. Je remercie tous ceux qui les ont partagés.

Merci à Jacques, mon directeur de thèse, aux membres du jury pour leur sympathie et leur bienveillance. Merci à Marie, à Christian et à tous les amis du labo qui m'ont soutenu, fait confiance et apporté joie et bonne humeur.

Merci aux «anciens» : Eric, Manu, David, Jeff, Luba, Fred, Vincent, Jean, Maël, Cat, Carole, Osho, Fadwa, Jean-Marie, Susana... aux «nouveaux» : Claire, Oscar, Fred, Seb, Felix, Hélène, Sémir, Hocine, Cédric ...

Je remercie ma famille et bien sûr merci (et pardon) à ceux que j'oublie.

A Mehdi

Table des matières

Introduction

Avec l'apparition et le développement des nouvelles technologies numériques, les fraudes se sont multipliées, soulignant le manque de méthodes concernant la protection des données numériques. Ces données sont en effet très faciles à pirater : on peut les stocker, les copier, les modifier et enfin les diffuser illégalement sans qu'elles perdent de leur qualité. Une image numérique, diffusée par exemple sur Internet, peut être aisément copiée puis rediffusée sur un réseau ou stockée sur CD-ROM sans prise en compte des droits d'auteurs. Pour répondre à ces besoins, un nouvel axe de recherche se développe très rapidement : le *tatouage* ou *watermarking*. Le principe des techniques dites de tatouage est d'insérer une marque imperceptible dans les valeurs de la donnée. Dans le cadre de la protection des droits d'auteurs, la marque insérée, appelée «watermarque» correspond au code du copyright. Ce type de tatouage doit répondre à des contraintes fortes en termes de robustesse. En effet, quelles que soient les transformations (licites ou illicites) que la donnée tatouée subit, la marque doit rester présente tant que la donnée reste exploitable. De plus, la présence de la marque ne doit être détectée que par des personnes autorisées (possédant une clef de détection privée). De nombreux algorithmes ont étés présentés récemment et certains produits sont même commercialisés, cependant, aucun d'eux ne satisfait pleinement au cahier des charges idéal.

Le travail présenté dans ce rapport a pour objectif de proposer une nouvelle méthode de tatouage des images numériques fondée sur la décomposition en paquets d'ondelettes. Le principe est d'imposer une structure (fixée par la marque) à la meilleure base, sélectionnée selon un certain critère énergétique, de l'image traitée.

Dans une première partie, nous exposons les principes et propriétés générales des processus de tatouage puis nous donnons un aperçu des techniques développées jusqu'à présent. Nous faisons la distinction entre les méthodes dites additives et les méthodes dites «virtuelles». Dans le premier type de techniques, la marque est ajoutée à des caractéristiques de l'image, dans des domaines spatiaux ou transformés. Dans le second, les valeurs de la marque dictent une contrainte que certains coefficients de l'image doivent respecter. Après avoir étudié les avantages et inconvénients des deux types de méthodes, nous choisissons de développer une technique de tatouage fondée sur le deuxième principe.

La deuxième partie du rapport présente les outils que nous utilisons : la transformée en ondelettes discrète, puis sa généralisation : la décomposition en paquets d'ondelettes. Cette transformation redondante du signal permet une décomposition sur plusieurs bandes fréquentielles suivant différents niveaux de résolutions. La redondance de

l'information contenue dans la décomposition en paquets d'ondelettes permet de choisir différentes bases de représentation du signal. Le choix d'une «meilleure» base est effectué en fonction du signal traité et d'un critère défini selon l'application voulue. Il existe différents algorithmes de sélection de meilleure base pour les applications telles que la compression, le débruitage, la classification et la détection de ruptures fréquentielles. Après les avoir présentés, nous détaillons l'algorithme de sélection de meilleure base que nous avons mis en place dans le cadre du tatouage d'images.

La troisième partie de ce rapport présente les différentes étapes nécessaires à la mise en oeuvre de notre algorithme de tatouage. L'étape d'implémentation de la marque consiste dans un premier temps à calculer la meilleure base de l'image selon le critère approprié. Cette structure nous permet d'accéder à la répartition spatio-fréquentielle de l'énergie de l'image. Les modifications du tatouage utilisent le fait que les paquets d'ondelettes portent une information spatiale et fréquentielle et minimisent la distorsion en norme L_2. L'étape de détection est aveugle : elle consiste à extraire une marque d'une image à l'aide de la clef privée de détection.

La partie suivante vise à améliorer notre méthode. Le tatouage reposant sur la structure de la meilleure base, une contrainte forte de notre méthode est la stabilité de la structure de la meilleure base face à diverses attaques. Nous analysons ainsi sur un ensemble d'images les réactions de la structure de la meilleure base face à un ensemble de transformations. Nous proposons ensuite une méthode visant à la stabiliser, puis nous fournissons une étude stochastique permettant d'optimiser la recherche de la meilleure base. Enfin, nous nous intéressons à la contrainte de non-perceptibilité du marquage. Nous contraignons les modifications faîtes à l'image selon un critère psychovisuel. Le dernier chapitre de cette partie consiste en l'étude d'un outil très utilisé en tatouage d'image : les m-séquences.

La cinquième partie de ce rapport produit une étude analytique de la méthode. Nous étudions en particulier les attaques illicites que peuvent faire les pirates afin d'invalider la détection de la marque. Nous proposons alors une méthode de tatouage à deux niveaux composée d'un tatouage public fragile et d'un tatouage privé robuste. Enfin, nous présentons une analyse critique portant sur la fiabilité des algorithmes de tatouage.

La dernière partie conclut notre travail en présentant les résultats de la méthode de tatouage proposée.

Première partie

Tatouage des images digitales pour la protection du copyright

Chapitre 1

Définitions et Propriétés générales des processus de tatouage d'images numériques

Le *tatouage* des données numériques est une discipline récente qui trouve son origine dans le manque de techniques fiables de protections de ce type de données. En effet, associé à d'autres techniques, cet axe de recherche a pour but de résoudre des problèmes aussi variés que la protection du copyright et des droits d'auteurs, la réglementation des copies, la prévention de la redistribution non autorisée, le suivi de documents et l'intégrité du contenu d'une donnée. Les différentes applications citées ci-dessus entraînent diverses contraintes qui seront détaillées dans le paragraphe 1.5. Nous ne développerons dans la suite de ce rapport que la partie du tatouage ayant trait à la protection du copyright et des droits d'auteurs des images numériques. Les propos généraux peuvent cependant s'étendre aux autres supports (audio ou vidéo). Après avoir présenté les premières définitions et propriétés du tatouage, nous définirons les processus d'implémentation puis de détection de la marque. Nous présenterons alors des techniques permettant d'évaluer une méthode de tatouage, puis nous donnerons les différentes applications de ces méthodes.

1.1 Principes généraux d'une méthode de tatouage pour la protection du copyright

L'objectif du tatouage pour la protection du copyright est d'introduire dans une image originale une marque invisible, appelée *watermarque* ou *filigrane*, contenant un code de copyright. L'image ainsi marquée ou *tatouée* peut alors être distribuée, elle portera toujours la marque de son propriétaire. Cette image est susceptible de subir diverses transformations. Ces transformations peuvent être licites (comme la compression) ou illicites, elles ont alors pour but de détruire le marquage. Si elles ne dégradent pas trop la qualité de l'image, ces modifications ne doivent pas gêner la détection de la marque : Le processus de tatouage est alors qualifié de *robuste* à ces *attaques*.

Dans la plupart des algorithmes de tatouage, le marquage est protégé par un code secret. Seules les personnes ou les organismes autorisés peuvent savoir si une image a été marquée et le cas échéant lire cette marque. Cette exigence se concrétise dans les algorithmes de tatouage par l'usage d'une clef privée cryptographique appartenant au propriétaire de l'image.

La définition la plus globale que l'on puisse donner d'une méthode de tatouage est la suivante

Définition 1 *Le principe général d'une méthode de tatouage d'une donnée numérique consiste à transmettre un message en même temps que la donnée, en modifiant directement la valeur des échantillons de cette donnée.*

Cette définition est intéressante car elle recouvre toutes les méthodes de tatouages, quelles que soient leurs applications. On remarque aussi que ces méthodes sont voisines de la discipline de la *stéganographie*[1]. On souligne ainsi les rapports du tatouage avec la théorie de la communication.

Appliquée au tatouage d'image pour la protection du copyright, et avec le vocabulaire introduit ci-dessus cette définition peut être reformulée de la manière suivante :

Définition 2 *Le principe général d'une méthode de tatouage d'une image numérique en vue de la protection du copyright consiste à transmettre une information de copyright en même temps que l'image, en modifiant imperceptiblement la valeur des échantillons de cette image. La détection de l'information de copyright doit être possible tant que l'image transmise est de qualité proche de celle de l'image originale. La mise en oeuvre de la détection doit nécessiter l'emploi d'une clef privée.*

Nous présentons figure 1.1 un schéma illustrant la définition 2. Le signal d'entrée I, appelé signal *hôte* sera modifié par une application $\mathcal{E}$. Cette étape est l'incrustation de la marque W dans I, avec l'intervention de la clef privée K. Le signal sortant I^*, est diffusé. Il est alors soumis à des transformations licites ou illicites de nature inconnue, cette version attaquée est notée I'. A la détection $\mathcal{D}$, la marque est extraite (on obtient alors une marque W') ou sa présence est contrôlée (une variable booléenne indique si la marque est présente dans l'image testée). Tous les processus de détection n'ont pas les mêmes entrées. Le paragraphe 1.3.1 présente les différentes versions de ce processus et la terminologie associée.

Nous allons maintenant présenter plus en détail les schémas d'implémentation et de détection de la marque. Nous accompagnerons ces schémas du formalisme donné par Petitcolas *et al.* dans [1] et généralement utilisé par la communauté des tatoueurs. Ils ont l'avantage de pouvoir modéliser tous les algorithmes de tatouage.

[1]La stéganographie du grec *steganos* (dissimulé) et *graphein* (écrire) se définit comme l'art de dissimuler un message. Contrairement au tatouage, le support (la donnée) n'a aucun lien avec le message. L'invisibilité est la contrainte principale des méthodes de stéganographie.

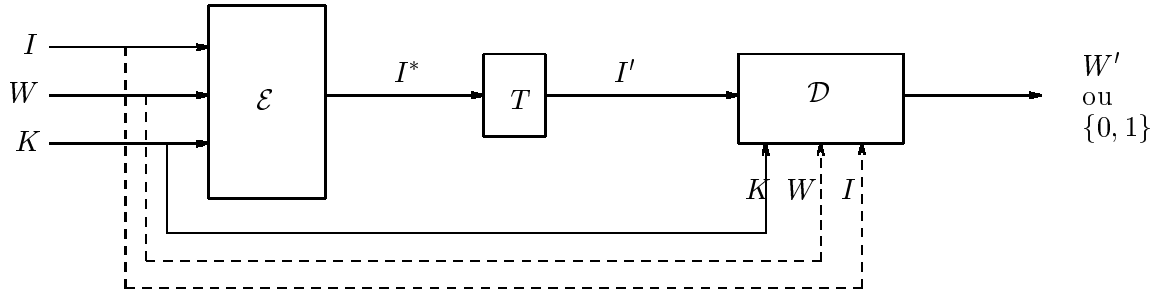


FIG. 1.1 – Schéma général d'un processus de tatouage. L'image tatouée I^* est obtenue par application de la fonction d'implémentation $\mathcal{E}$ sur la clef K, la marque W et l'image originale I. I^* subit alors des transformations T, l'image résultante est testée par un processus de détection $\mathcal{D}$, qui extrait la marque ou détecte sa présence.

1.2 Processus d'implémentation de la marque

Schéma général

La figure 1.2 présente le schéma général d'implémentation de la marque. Une image hôte I est tatouée d'une marque W par un propriétaire possédant une clef privée K. L'image résultat I^* est perceptuellement similaire à I et contient le code de copyright W.

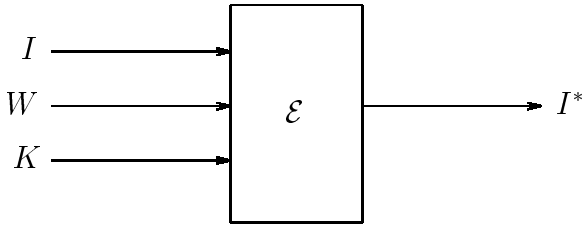


FIG. 1.2 – Schéma général du processus d'implémentation d'une marque. I est l'image hôte, K la clef privée, W la watermarque, I^* est l'image tatouée résultat de l'application $\mathcal{E}$

Formalisme

L'implémentation de la marque est une application $\mathcal{E}$ de l'espace des clefs $\mathcal{K}$, de l'espace des marques $\mathcal{W}$ et de l'espace des images $\mathcal{I}$ dans ce dernier espace. Elle fait correspondre à une clef K, une watermarque W et une image hôte I, une image tatouée I^*.

$$\begin{array}{rcl}(\mathcal{W},\mathcal{K},\mathcal{I}) & \longmapsto & \mathcal{I} \\ (W,K,I) & \longmapsto & I^*\end{array} \tag{1.1}$$

Ce formalisme, très général, représente le processus d'implémentation de la marque pour tous les processus de tatouage. Nous allons maintenant préciser les propriétés que

l'application $\mathcal{E}$ doit satisfaire et définir les espaces de départ et d'arrivée $\mathcal{W}, \mathcal{K}$ et $\mathcal{I}$.

1.2.1 La fonction d'implémentation

Contrainte d'imperceptibilité

Le marquage doit être imperceptible, c'est à dire qu'un utilisateur quelconque ne doit pas pouvoir différencier visuellement l'image marquée de l'image originale. Cette propriété est importante pour deux raisons. La première est évidente : le marquage ne doit pas empêcher la compréhension de l'oeuvre, celle-ci doit garder toute sa qualité artistique ou commerciale. Une autre raison est, qu'ainsi cachée, la marque est plus difficilement détruite par piratage.

Dans la plupart des algorithmes proposés, l'imperceptibilité du tatouage s'obtient en utilisant diverses propriétés du Système Visuel Humain (SVH). Ces propriétés, souvent trouvées à partir d'heuristiques, proposent des modélisations du comportement psychovisuel humain. Le paragraphe 2.1.3 présente les principes d'un tatouage psychovisuel. En général, un seuil de perceptibilité est calculé à partir de l'image originale, les modifications de l'image ne peuvent se faire qu'à concurrence de ce seuil.

Cette contrainte pose un problème d'évaluation. En effet, une fois l'image tatouée, on doit pouvoir assurer que les distorsions causées sont imperceptibles. On utilise couramment le $PSNR$ (pour Peak Signal to noise Ratio) pour quantifier ces dégradations. Nous expliquerons paragraphe 1.4.1 que cette mesure n'est pas adaptée à notre propos.

Sûreté du tatouage, inversibilité de $\mathcal{E}$

Comme dans toutes les disciplines proches de la cryptographie, la sûreté du système est assurée uniquement par la confidentialité de la clef K. En effet, on ne peut pas garantir la confidentialité des algorithmes mis en oeuvre. Cette exigence correspond au deuxième principe de Kerckhoffs [2]. Si K est inconnu, aucun utilisateur ne doit pouvoir retrouver l'image originale. Cette contrainte est souvent remplacée par la suivante, plus réaliste : Ne connaissant pas la clef secrète, un pirate ne doit pas pouvoir retrouver l'image originale sans pour cela mettre en oeuvre des moyens plus coûteux que ceux correspondant à l'achat des droits de copyright.

L'*inversibilité* de l'application $\mathcal{E}$ est donc conditionnée par la connaissance de la clef. Cette inversibilité n'est pas obligatoire. Elle peut être recherchée si les ayant-droits de l'image veulent enlever la marque pour en ajouter une autre (si par exemple, le statut de copyright a changé). L'inversibilité de $\mathcal{E}$ est impossible si des informations inhérentes à l'image originale ont disparu dans la version tatouée. Certains processus d'implémentation sont par exemple fondés sur une substitution ou une quantification des valeurs de l'image qui sont alors irrémédiablement modifiées. Ces derniers schémas assurent plus de sécurité dans le cas où la clef est divulguée et peuvent alors servir pour des algorithmes dits à clef publique, où aucun secret n'est requis pour la détection de la marque [3].

Remarque : L'inversibilité est comprise ici en son sens mathématique (certains auteurs l'appellent réversibilité). En tatouage d'images, le terme d'inversibilité est souvent employé pour définir une attaque, appelée *dead lock attack* ou *impasse*. Nous verrons dans le paragraphe suivant que cette attaque, proposée par Craver *et al.* [4], utilise un défaut d'*injectivité* de l'application $\mathcal{E}$.

Injectivité de l'application $\mathcal{E}$

Si une image marquée correspond à deux propriétaires différents, c'est à dire deux couples (W, K), on se retrouve dans la position dite de l'impasse : On ne peut pas conclure sur l'appartenance de l'image à l'un ou l'autre des propriétaires. Cette situation arrive si l'application $\mathcal{E}$ n'est pas injective.

Craver *and al.* [4] ont utilisé un défaut d'injectivité de la fonction $\mathcal{E}$ pour invalider le processus de marquage. A partir d'une image tatouée, $I^* = \mathcal{E}(W_A, K_A, I_A)$, un attaquant, exhibe un triplet (W_B, K_B, I_B) tel que $I^* = \mathcal{E}(W_B, K_B, I_B)$. Cette attaque invalide le processus de marquage, puisque, quelque soit la méthode de détection, le double marquage est présent, on ne peut pas conclure quand à la propriété de l'image.

La solution proposée pour éviter ce problème est de restreindre les espaces de départs (cf. paragraphe 1.2.2) en imposant une structure fixée à la clef et à la marque. Si on impose de plus que la clef soit fonction de l'image originale, l'attaquant aura alors beaucoup plus de mal à générer le triplet solution (W_B, K_B, I_B). En général, un tiers de confiance intervient dans le protocole de tatouage, il délivre par exemple la clef privée, pour chaque image.

Surjectivité de l'application $\mathcal{E}$

$\mathcal{E}$ est surjective si et seulement si, il existe pour toute image I, un triplet (W_A, K_A, I_A) tel que $I = \mathcal{E}(W_A, K_A, I_A)$. Pour notre application, ceci signifie que toutes les images (originales ou non) possèdent une marque à l'état naturel. Il suffirait à un pirate de trouver le code et la marque pour s'approprier les images originales en circulation. Le danger de cette attaque, très proche de celle mentionnée ci-dessus est évité de la même manière : On restreint les ensembles de départs et on introduit un tiers de confiance dans le protocole de tatouage.

Conclusion

Si l'on veut donner un formalisme mathématique rigoureux de l'application $\mathcal{E}$, les deux contraintes d'injectivité et de surjectivité présentées ci-dessus imposent de redéfinir les ensembles de départs et d'arrivée de cette application. Soit $\mathcal{I}_o$ l'ensemble des images originales et $\mathcal{I}_m$, l'ensemble des images tatouées. L'application $\mathcal{E}$ est alors définie comme une injection de l'espace d'entrée sur l'espace de sortie :

$$\begin{array}{rcl} (\mathcal{W}, \mathcal{K}, \mathcal{I}_o) & \longmapsto & \mathcal{I}_m \\ (W, K, I) & \longmapsto & I^* \end{array}$$

Cette définition est impossible à utiliser pratiquement, l'espace $\mathcal{I}_o$ ne peut en effet être ni défini ni connu, il est en constant changement. Nous garderons donc comme définition de l'application $\mathcal{E}$ celle donnée dans 1.1. Les solutions envisagées pour résoudre les situations explicitées ci-dessus seront d'ordre protocolaires. On considérera par la suite que le processus de tatouage est associé à un modèle fonctionnel et que les clefs sont distribuées par un tiers de confiance.

Nous allons maintenant définir plus précisément ce que représentent les espaces d'entrées et de sorties du processus, c'est à dire l'espace des marques, celui des clefs, puis nous parlerons des images.

1.2.2 Espaces d'entrées

Espace des watermarques

L'ensemble $\mathcal{W}$ est l'ensemble de toutes les marques possibles. Son cardinal doit être le plus grand possible, c'est à dire que la longueur de la marque W doit être la plus grande possible. Cette longueur est pourtant limitée par plusieurs contraintes. D'une part, elle dépend de la taille de l'image hôte. En effet, on ne peut pas inscrire trop d'informations dans un petit support. De plus, la contrainte d'invisibilité impose une marque de petite taille. Il est évident que plus la marque est petite, plus il est facile de la cacher. Enfin, pour assurer la robustesse du processus de tatouage, W est fortement redondant. Cette redondance s'exprime de plusieurs manières, ce peut être de la redondance pure (la même information est répétée plusieurs fois), l'emploi de code correcteur d'erreurs ou l'emploi de techniques dites d'étalement de spectre (voir 2.1.1). Dans certains algorithmes, la marque a une structure prédéfinie, comme par exemple une succession de M-séquences. La taille de la marque est ainsi toujours supérieure à celle de l'information qu'elle porte.

Pour l'instant aucune norme n'a été adoptée concernant la taille de chaque marque et donc le cardinal de l'ensemble $\mathcal{W}$. Dans la plupart des contributions, la marque est fixée à une centaine de bits pour une image 512×512 codée sous 8 bits.

Dans certaines méthodes dites additives à étalement de spectre (voir paragraphe 2.1.1), la présence de la marque est détectée sur 1 bit. L'algorithme de détection signale uniquement la présence d'un motif correspondant à un tatouage de l'image. Ce motif dépendant de la clef K, c'est la connaissance de cette clef qui joue le rôle d'identifiant. Il faut alors que le cardinal de $\mathcal{K}$ soit très grand, pour caractériser le maximum de propriétaires.

Espace des clefs

C'est sur la connaissance de la clef K que repose toute la sécurité du marquage. En effet si K est divulguée, tout le monde peut détecter et lire la marque. Dans la plupart des schémas à clef privée, la connaissance de la clef permet de retrouver l'image originale ou d'invalider la détection du tatouage. Ainsi, un pirate ne doit pas pouvoir retrouver la clef. Toute tentative de recherche exhaustive de la clef doit être impossible ou trop coûteuse à réaliser. Pour cela, la taille de la clef doit être grande et sa structure

compliquée. Inversement, la clef privée doit être facilement stockée par le propriétaire et le tiers de confiance, sa taille doit donc être raisonnable. Si par exemple, la taille de la clef est proche de celle de l'image originale, le tatouage pour la protection du copyright n'a plus lieu d'être : il serait alors plus simple que le tiers de confiance stocke directement l'image originale.

K est issue d'un processus cryptographique, nous ne nous intéresserons pas ici à sa conception et son codage, nous nous contenterons de définir les informations qu'elle contient. Par exemple, des schémas de tatouage utilisent cette clef pour piloter les endroits où la watermarque est implémentée. Dans d'autres schémas dits à étalement de spectre (voir paragraphe 2.1.1), la clef génère un motif qui sera vecteur de la marque.

L'ensemble des images hôtes

A priori, n'importe quelle image doit pouvoir être tatouée. Cependant, il est évident qu'on ne peut pas marquer les images de trop petite taille (quelques pixels sont insuffisants pour contenir la marque). En général, les processus de tatouage fixent la taille minimale des images hôtes à 512×512 pixels ou plus rarement à 256×256 pixels. Ce dernier choix paraît raisonnable puisque les industriels appellent les images de 256×256 pixels «imagettes» et ne leur confèrent pas de valeur commerciale. Les schémas de tatouage excluent donc de l'espace des images hôtes les images de petite taille. Cette restriction de l'espace de départ entraîne des problèmes de robustesse. Nous verrons au paragraphe 1.4.2 qu'une attaque appelée attaque de *mosaïque* utilise cette restriction pour invalider la détection du marquage.

Afin de pouvoir cacher la marque, il est clair que le support doit respecter d'autres contraintes, si par exemple l'image est trop monotone, le schéma d'implantation de la marque ne pourra pas fonctionner ou le tatouage sera trop visible. C'est le problème posé par certaines images synthétiques comme les dessins qui contiennent de grandes zones uniformes. Les applications concernant les images médicales commencent à être étudiées spécifiquement. La plupart des schémas de tatouage s'intéressent cependant à des images hôtes de type «cinéma» ou photographie. Celles-ci représentent en effet la majorité des images en circulation.

Formellement, une image est une application I de l'espace des coordonnées spatiales dans un ensemble de valeurs quantifiées : à chaque couple de coordonnées (x, y) de l'image (appelé usuellement pixel), on associe une valeur $I(x, y)$. Selon les modes de représentation, la valeur d'un pixel peut être exprimée de différentes façons : pour les images couleurs, la valeur d'un pixel est contenue dans un triplet (R, G, B) ou (Y, U, V). Dans la première représentation, R désigne la quantité de rouge, G celle de vert et B celle de bleu, dans la seconde, Y est la luminance du pixel, U et V étant des paramètres de chrominance. Les images dites à niveau de gris ne sont représentées que par les valeurs de luminance Y. Le système visuel humain étant moins sensible à la luminance qu'aux chrominances, les algorithmes de tatouage ne modifient que ce paramètre. On ne travaillera ainsi que sur des images à niveaux de gris, les résultats étant transposables aux images en couleurs.

1.3 Processus de détection de la marque

Schéma général

La figure 1.3 présente le schéma général de détection $\mathcal{D}$ de la marque. L'entrée du processus est constituée d'une image test I' et de la clef K de détection. Certains algorithmes nécessitent en plus la connaissance de l'image originale I et de la marque implantée W (en pointillés sur le schéma). La sortie du détecteur peut être la watermarque extraite W' ou un résultat de décision indiquant si la marque W a été retrouvée dans I'.

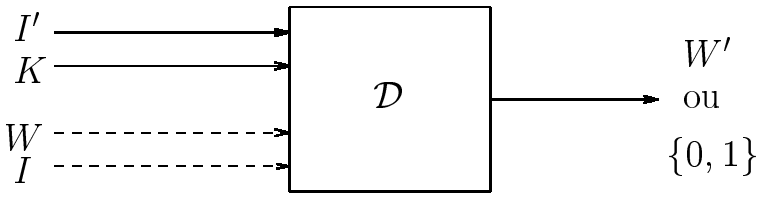


FIG. 1.3 – Schéma général du processus de détection d'une marque. I' est l'image test, K la clef privée, W la watermarque, I est l'image originale. Le résultat de la détection $\mathcal{D}$ peut être une marque ou une décision

1.3.1 Formalisme des différents types de détection

Nous avons vu dans la présentation du schéma général du processus de détection que les entrées et les sorties du système peuvent varier selon les algorithmes. Nous allons ici nommer et caractériser ces différents processus.

Les schémas privés La détection est dite *privée* si l'image originale est nécessaire.

– Si le détecteur extrait la marque, il est dit de *Type I*, on a alors :

$$(K, I, I') \longmapsto W'$$

– Si le détecteur est une mesure de présence de la marque (sa sortie sera 1 si la marque est détectée 0 sinon), la détection est alors une application de *type II* avec :

$$(W, K, I, I') \longmapsto 0, 1$$

La présence de l'image originale à la détection facilite la création du schéma général de tatouage (implémentation et détection) et apporte beaucoup de robustesse à ce schéma. Cependant, ceux ci ne sont pas adaptés à toutes les applications pour des raisons évidentes (comme dans le cas de la réglementation de copies) ou des raisons techniques (comme dans le cas du suivi de document). Ils sont en fait utilisés dans des cas très particuliers (voir paragraphe 1.5).

Les schémas semi-privés Une détection *semi-privée* n'utilise pas l'image originale et donne une réponse sur la présence de la marque

$$(W, K, I') \longmapsto 0, 1 \tag{1.2}$$

Les schémas aveugles Une détection *aveugle* (appelée parfois publique) extrait la watermarque insérée sans l'image originale.

$$(K, I') \longmapsto W$$

La robustesse du schéma ne repose ici que sur la connaissance de la clef, on ne peut plus s'appuyer sur le caractère privée de la connaissance de l'original ou de la marque : il faut donc apporter beaucoup de soin à anticiper les attaques possibles. Ce schéma est utilisable dans tous les cas de tatouage nécessitant une clef privée.

Les schémas asymétriques La détection par algorithmes *asymétriques ou à clef publique* peut être schématisée comme une détection aveugle, la clef secrète de détection étant connue de tous. Une des principales difficultés de ce type de tatouage est d'empêcher la destruction de la marque ou son invalidation alors que tous les utilisateurs connaissent l'algorithme employé et la clef. C'est pour cela que l'on utilise des algorithmes asymétriques où la clef d'implantation de la marque n'est pas la clef de détection.

Commentaires Pour la protection du copyright, la marque est supposée connue, les algorithmes de détection par extraction sont alors suivis d'une étape de vérification. La figure 1.4 présente cette détection globale. La marque extraite W' est comparée à une marque prédéfinie W par mesure de corrélation ou par mesure de distance de Hamming. Cette mesure est finalement seuillée pour obtenir la valeur de décision : 1 si l'image I' est considérée tatouée, 0 sinon.

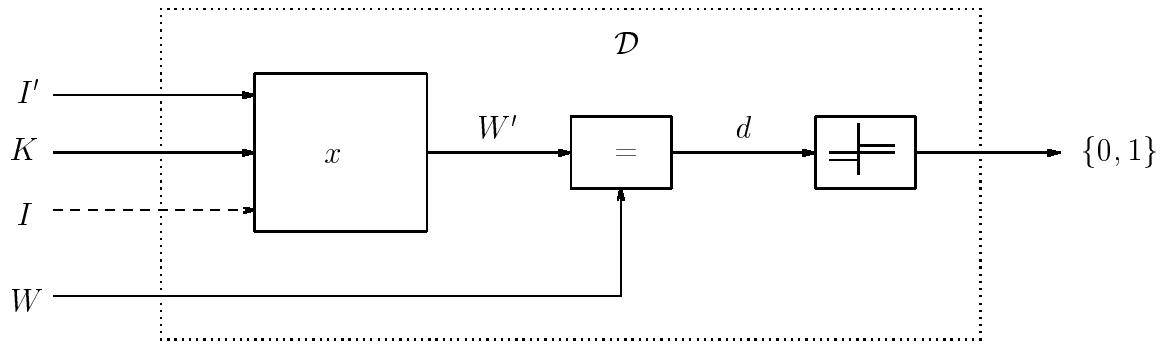


FIG. 1.4 – Schéma général du processus de détection par extraction x de la marque W' puis comparaison avec la marque prédéfinie W puis enfin seuillage du résultat pour obtenir la valeur de décision.

Dans la suite de ce rapport, nous nous appuierons sur le formalisme des schémas semi-privés (voir la relation 1.2).

1.3.2 Propriétés du processus de détection

Robustesse aux attaques

Une fois tatouées, les images diffusées peuvent être soumises à des transformations quelconques. Ces transformations, qu'elles soient licites ou illicites, constituent des attaques sur le processus de tatouage. Le paragraphe 1.4.2 donne des exemples d'attaques possibles. Si ces attaques ne dégradent pas trop la qualité de l'image, elles ne doivent pas gêner la détection de la marque, le détecteur est dit robuste à ces attaques.

Soit t une transformation quelconque de l'image, soit I^* une image tatouée de la marque W avec la clef K, on peut formaliser la contrainte de détection par la définition suivante :

$$\text{Si} \quad t(I^*) \sim I^* \tag{1.3}$$
$$\text{alors} \quad \mathcal{D}(W, K, t(I^*)) = 1 \tag{1.4}$$

où $\sim$ est l'opérateur «similarité perceptuelle» : $A \sim B$ signifie que les images A et B se ressemblent et qu'aucune ne paraît dériver de l'autre.

Cette définition pose deux problèmes techniques, le premier est qu'on n'a aucune connaissance à priori sur l'attaque t, la seconde est la difficulté d'évaluation de la similarité perceptuelle.

Sûreté de la détection

Conformément au principe de Kerckhoffs, la connaissance de l'algorithme de détection utilisé ne doit pas permettre de retrouver la clef K. En effet, c'est sur la confidentialité de cette information que repose le protocole de tatouage.

Fiabilité de la détection

Un processus de détection fiable doit minimiser la probabilité de faux négatifs (une marque présente n'est pas détectée) et interdire les probabilités de fausses alarmes (une marque est détectée à tort). Pour toute transformation t, on peut noter la probabilité de faux négatifs :

$$P_{fn} = P(D(W, K, I') = 0 | \quad I' = t(I^*), \quad I' \sim I^*) \tag{1.5}$$

et de même la probabilité de faux positifs :

$$P_{fa} = P(D(W, K, I') = 1 | \quad I' \neq t(I^*)) \tag{1.6}$$

avec $P(A|B)$ signifiant «probabilité de A sachant B». Ces deux probabilités sont appelées respectivement probabilités d'erreurs de type I et de type II.

1.4 Évaluation des algorithmes de tatouage

Évaluer les processus de tatouage n'est pas une chose immédiate. Nous avons vu qu'aucun cahier des charges ne donne des valeurs fixées pour la longueur de la marque, la qualité du tatouage (son imperceptibilité) ou l'ensemble des attaques auxquelles le tatouage doit être robuste.

1.4.1 Qualité

La notion de qualité intervient deux fois dans le cahier des charges d'un processus de tatouage. Il faut d'une part que l'image tatouée soit de la même qualité que l'image originale, c'est le critère d'imperceptibilité du tatouage présenté au paragraphe 1.2.1. D'autre part, les attaques auxquelles doit être robuste le tatouage, doivent conserver la qualité de l'image, comme le précise l'équation 1.3. Cette notion de qualité permet donc de caractériser les attaques et de restreindre leur ensemble afin d'étudier la robustesse de la marque.

Mesure de la qualité d'une image

La première constatation est qu'il n'existe aucune méthode automatique pour mesurer la qualité absolue d'une image. Aucun algorithme n'est capable, sans image de référence, de dire qu'une image est de bonne ou mauvaise qualité. Cependant, dans le cadre de nos applications, cette contrainte n'est pas restrictive puisque l'image originale peut nous servir de référence. La mesure de qualité des images est donc une mesure de distance entre deux images.

Les mesures de distances les plus simples comparent les deux images pixels par pixels. Ces diverses mesures de distorsions sont regroupées dans le tableau page 4 de l'article [5]. Elles sont fondées sur la différence entre les deux images ou sur des corrélations entre ces images. Les mesures de distorsion les plus populaire en traitement d'image et compression étant tout simplement le rapport signal sur bruit (SNR Signal to Noise Ratio) et le (PSNR Peak Signal to Noise Ratio). Ils sont mesurés en décibel (dB) à partir des relations suivantes :

$$(SNR)_{dB} = 10\log_{10}(\sum_{m,n} I_{m,n}^2 / \sum_{m,n}(I_{m,n} - \tilde{I}_{m,n})^2) \tag{1.7}$$

$$(PSNR)_{dB} = 10\log_{10}(MN \max_{m,n} I_{m,n}^2 / \sum_{m,n}(I_{m,n} - \tilde{I}_{m,n})^2) \tag{1.8}$$

où $I(m,n)$ est la valeur du pixel (m,n) de l'image référence et $\tilde{I}(m,n)$ celle de l'image à tester, les deux images étant de taille $[M \times N]$.

Si ces mesures quantifient bien les dégradations par ajout de bruit, leurs applications dans notre cadre de travail pose différents problèmes. Les plus évidents concernent par exemple les transformations affines : Si on fait subir une symétrie à une image, le PSNR

entre l'image modifiée et son original pourra être très bas alors que l'image n'est pas modifiée. On ne peut donc pas utiliser ces mesures de manière systématique.

On peut observer aussi que ces mesures n'intègrent pas dans le calcul les comportement des voisinages des pixels traités, et qu'aucun comportement fréquentiel n'est pris en compte. Enfin, aucun critère psychovisuel n'est utilisé. On utilisera cependant le PSNR comme valeur indicative. On sait par exemple qu'une image de PSNR inférieure à 35 dB sera probablement de mauvaise qualité.

La qualité des images peut s'obtenir à partir de critères subjectifs. La recommandation 500 du CCIR [6] propose de présenter les images modifiées et originales à un groupe d'observateurs composé d'experts et de non-spécialistes. On présente les images à deux moments distincts, la distance de présentation requise est de quatre fois la hauteur de l'écran. Les appréciations possibles de la qualité de l'image sont réunie dans le tableau 1.1.

TAB. 1.1 – Notes de qualité des images

NOTE	QUALITÉ
5	Excellente
4	Bonne
3	Assez Bonne
2	Médiocre
1	Mauvaise

Cette mesure de qualité subjective est intéressante et peut servir de test final pour mesurer la qualité du tatouage. Elle ne peut évidemment servir ni de test systématique, ni de critère aidant à la construction d'un schéma de tatouage ou d'une attaque.

Différents outils psychovisuels permettant de noter la qualité d'une image dégradée par rapport à une image originale existent dans la littérature [7] [8]. Ces méthodes sont très proches de celles utilisées en tatouage psychovisuel, elles sont basées sur les mêmes modélisations du Système Visuel Humain (SVH). On peut, en utilisant ces méthodes, assurer qu'une image est excellente. Cependant, la caractérisation des 4 autres degrés de qualité est plus complexe et de nombreuses études sont menées actuellement sur le sujet.

Compromis invisibilité-robustesse

Dans tous les algorithmes de tatouage apparaît un coefficient appelé *force* du tatouage. Schématiquement, pour un algorithme à insertion spatiale : $I^* = I + \alpha W$, la force du marquage est le coefficient α. Il est clair que ce coefficient intervient directement dans les performances de robustesse du schéma. Plus le marquage est «fort», plus il est visible et plus il est robuste à certaines attaques (comme l'ajout de bruit).

Le compromis proposé par les schémas de tatouage utilisant des critères psychovisuels est de calculer le coefficient maximum $\alpha(i,j)$ pour chaque pixel de coordonnées (i,j). Les dégradations de marquage seront alors juste à la limite de perceptibilité hu-

maine. Nous utiliserons au paragraphe 11 des critères psychovisuels permettant d'assurer l'imperceptibilité de notre méthode de tatouage.

1.4.2 Attaques

Les attaques tiennent une place très importante dans le cahier des charges d'un processus de tatouage puisqu'elles définissent la robustesse d'un système. Une façon simple de classer les attaques serait de quantifier les dégradations qu'elles font subir à l'image. Ceci permet de vérifier directement que le cahier des charges est respecté. Nous avons vu ci-dessus les problèmes posés par la caractérisation de la qualité d'une image. Nous n'avons pas pour le moment de critère assez performant pour classer les attaques de cette façon.

Classiquement, on peut séparer les attaques de la manière suivante. Les transformations usuelles de l'image comme la compression, ne visent pas forcément à attaquer le tatouage, ce sont des attaques non-intentionnelles. Le deuxième groupe d'attaques est constitué des attaques «génériques», *i.e* qui ne visent pas un algorithme en particulier. Le troisième ensemble concerne les attaques ciblées sur une méthode de tatouage déterminée. Enfin, les dernières attaques invalident les protocoles associés au tatouage, comme par exemple l'attaque de l'impasse.

Une autre idée est d'étudier les attaques selon l'étape du tatouage qu'elle mettent en défaut. En effet, si des pirates tentent par exemple d'enlever la marque, c'est l'étape d'implémentation qui est visée. Ils peuvent aussi vouloir invalider le marquage, en noyant par exemple le message dans du bruit, c'est alors l'étape de détection qui est visée. Le tableau 1.2 donne une classification des diverses attaques selon cette distinction. Nous allons maintenant détailler certaines de ces attaques et donner si possible des solutions pour leur résister.

TAB. 1.2 – Classifications des attaques

Attaques sur l'implémentation	Attaques sur la détection
cropping	applications affines
filtrage	ajout de bruit
compression	jitter attack
débruitage	passage à l'analogique
moyennage	Stirmark
impasse	Unsign
	mosaïque
	collusion
	surmarquage
	copiage
	fausses alarmes naturelles

Les attaques du processus d'implémentation de la marque

Faire le **cropping** d'une image consiste à en extraire un morceau. Pour être résistant à ce type d'attaque, le tatouage doit être présent sur toute l'image. La même situation se produit dans le domaine fréquentiel de l'image où la marque doit être partout présente afin d'éviter une destruction par **filtrage** passe bande.

Les algorithmes de **compression** sont particulièrement dangereux pour les processus de tatouage puisque leur objectif est exactement l'opposé de celui du tatouage. On veut en effet, par l'utilisation de ces algorithmes ne garder de l'image que les composantes essentielles à leur compréhension (une marque invisible n'est évidement pas essentielle). C'est pourquoi Cox *et al* [9] proposent d'insérer la marque dans des endroits «perceptuellement significatifs » de l'image. Ces lieux de marquage seront souvent choisis directement dans les domaines transformés utilisés par les algorithmes de compression (voir le paragraphe 2.1.2).

La marque insérée dans l'image ressemble souvent à du bruit, c'est donc tout naturellement que les pirates appliquent au document marqué des méthodes classiques de **débruitage** (filtres de Wiener, filtre de Kalman, estimation du maximum a posteriori, ondelettes, multifractal) pour lui retrancher l'estimée de la marque. Sous certaines conditions, le signal résultant sera proche du signal original.

Ces attaques par cropping, filtrage, compression et débruitage font parties des attaques dites non-intentionnelles. Si un pirate utilise l'une d'elles, la principale difficulté qu'il rencontrera sera qu'il ne pourra pas savoir (ne disposant pas de la clef de détection) si cette attaque est une réussite.

Des méthodes plus complexes cherchent à retirer «chirurgicalement» la marque du signal tatoué. Cette opération peut être très facile dans un cas particulier : si l'implémentation de la marque ne dépend pas de l'image. Dans ce cas, un pirate possédant plusieurs images différentes contenant la même marque pourra enlever celle-ci. En effet, un simple **moyennage** des images donnera une estimée de la marque, qu'il pourra alors retrancher aux images tatouées. Cette situation peut par exemple avoir lieu si l'on marque une séquence de film. On imposera donc que l'étape d'implémentation de la marque soit dépendante de l'image, on dira que le tatouage est statistiquement imperceptible.

L'attaque de l'**impasse** inhibe directement le protocole de tatouage. Nous avons vu au paragraphe 1.2.1 que cette attaque est due à un défaut d'injectivité de l'application d'implémentation de la marque.

Les attaques du processus de détection de la marque

Une attaque très simple et très dangereuse pour la plupart des schémas de tatouage consiste à désynchroniser la transmission du document. Dans cette attaque, la marque est décalée, le détecteur ne la retrouve pas aux endroits attendus et conclut à l'absence de la marque. Pour la protection des images digitales, cette désynchronisation se fait la plupart du temps par le biais d'**applications affines**, telles que la translation ou la rotation. Nous verrons dans le chapitre suivant, lorsque nous détaillerons les différentes méthodes existantes, les remèdes à cette attaque. Le **passage du numérique à l'analogique** avec

retour au numérique constitue une attaque intéressante car c'est le moyen le plus évident de détourner des données payantes (chaînes de télévision à péage ...). Cette opération est souvent considérée comme composée de l'**ajout d'un bruit** et d'une attaque appelée en anglais **jitter attack** consistant à enlever des lignes et des colonnes et à en dupliquer d'autres.

Ces attaques bien que dangereuses n'ont pas été créees intentionnellement pour invalider le tatouage. Dans le logiciel **Stirmark** [5], il existe une attaque appelée du même nom qui consiste à appliquer des petites déformations géométriques invisibles sur l'image. Ces déformations désynchronisent le détecteur qui ne retrouve plus la marque (bien que celle-ci soit présente). **Unsign** [10] est un logiciel dont seuls les exécutables sont disponibles sur Internet, il permet également d'effectuer des déformations invisibles sur l'image afin de craquer une marque.

Une autre attaque proposée dans [11] permet d'invalider la détection sans pour autant supprimer la marque. Cette attaque utilise le fait qu'on ne peut pas tatouer d'images de trop petite taille. Un pirate appelé Bob vole une image appartenant à Alice[2] afin de la mettre sur son site Internet. Il décompose cette image en petites imagettes qu'il accole en **mosaïque** sur sa page Internet. Un utilisateur visitant le site de Bob verra l'image globale portant le tatouage d'Alice mais un robot traqueur équipé d'un détecteur ne reconnaîtra pas la watermarque. Cette attaque très simple est imparable.

L'attaque dite de **collusion** a lieu lorsque plusieurs utilisateurs sont en possession du même document portant différentes watermarques. La mise en commun de ces documents permet de nombreuses opérations : moyenne, recherche de propriétés statistiques communes dans différents domaines, recherche d'informations sur la localisation de la marque... Décrivons une attaque par moyenne : l'image résultante de la moyenne des images tatouées en circulation aura la même qualité que ces dernières. Elle contiendra toutes les marques, leurs amplitudes étant fortement diminuées. La détection sera alors perturbée à la fois par cette baisse d'amplitude et de possibles interférences entre les marques.

L'attaque par **surmarquage** consiste à tatouer à nouveau une image déjà tatouée. Pour certains schémas, en particulier si les lieux de tatouages sont fixés, cette attaque peut être très dangereuse. Certains protocoles de tatouage se protègent en vérifiant, avant de distribuer une clef, que l'image originale proposée n'est pas tatouée. Cette protection n'est utile que si le schéma de tatouage demeure inconnu. En effet, s'il est connu, un pirate peut ajouter une marque de sa fabrication qui invalidera la détection. L'image ne lui appartiendra pas (le tiers de confiance n'étant pas le distributeur de la clef) mais le pirate possédera une version non tatouée de l'image. Les protocoles se protégeant en distribuant uniquement des clefs pour les images non tatouées ne respectent donc pas le principe de Kerckhoffs. C'est le cas du processus de tatouage public de Digimarc [12]. De plus cette protection peut être contournée. C'est le principe d'une attaque [11] visant particulièrement l'algorithme de tatouage de Digimarc. Dans celle-ci, les pirates commencent par contourner l'interdiction au surtatouage : une image

[2]Dans les domaines proches de la cryptographie, les deux protagonistes sont appelés, par souci de clarté, Alice et Bob. dans notre cas, Alice est la propriétaire de l'image. Bob est le pirate.

est dégradée jusqu'à ce que l'on puisse la surtatouer (la première watermarque n'étant plus lisible). On ajoute à l'image originale l'image ainsi surtatouée (en diminuant son amplitude pour que les dégradations n'apparaissent plus). L'image résultante porte alors les deux tatouages, mais le détecteur n'en lit qu'un, le nouveau : le pirate s'est donc approprié l'image.

L'attaque par **copiage** consiste à recopier une marque obtenue préalablement (par exemple par estimation) sur une image non marquée. Le détecteur validera alors la nouvelle image comme étant tatouée. Cette attaque s'applique naturellement aux problèmes d'intégrité, puisqu'elle rend possible la présentation de faux qui seront authentifiés par le détecteur.

Un schéma de détection recherche un motif (la marque) présent dans l'image. Ce motif est soit implanté dans la donnée de façon licite (c'est le but de l'étape d'implémentation), soit de façon illicite comme pour l'attaque de copiage ou d'impasse, mais il peut aussi arriver que ce motif soit présent «à l'état naturel» dans une image originale. Les **fausses alarmes naturelles** déclenchées ainsi sont statistiquement très nombreuses et représentent un vrai problème pour l'intégrité des schémas de tatouage. Nous présenterons au paragraphe 15 les calculs de probabilité d'apparition de ces fausses alarmes pour plusieurs méthodes.

Conclusion

Nous n'avons pas fait ici une description exhaustive de toutes les attaques existantes. En particulier, nous n'avons pas présenté les attaques spécifiques à certains algorithmes. Cet aperçu nous a cependant permis de préciser certaines contraintes imposées au schéma d'implémentation : la marque, dépendante de l'image, doit recouvrir tout le domaine spatial et fréquentiel de celle-ci. Elle doit de plus modifier des composantes significatives de l'image hôte.

Les différentes attaques présentées ici montrent la nécessité de penser la conception de l'algorithme en termes d'applications : une fois ces applications définies, il devient possible d'anticiper les attaques qui seront utilisées et de les contrer. Une des conséquences de cette approche globale est d'accorder une grande importance à la détection : il ne suffit pas de placer la marque à un endroit du signal où elle sera particulièrement robuste, il faut aussi pouvoir la retrouver avec un faible risque d'erreur de détection. L'approche globale est particulièrement importante : si un maillon du schéma a été négligé et qu'il subit une attaque (concluante), le document ne pourra plus être protégé puisque des «versions originales» auront été diffusées numériquement en grande quantité.

1.4.3 Conclusion

Nous nous sommes intéressés dans ce paragraphe aux outils d'évaluation des algorithmes de tatouage. La première constatation est qu'on ne dispose pas d'outils fiables de mesure de qualité des images. La deuxième concerne l'ensemble des attaques : Une présentation des attaques possibles nous a permis de trouver de nouvelles contraintes

aux algorithmes d'implémentation. Mais surtout, notre attention s'est portée sur la nécessité de concevoir un algorithme en considérant une approche globale, c'est à dire en apportant un soin particulier à l'étape de détection de la marque et ceci dès la conception de l'étape d'implémentation. De plus, pour pouvoir anticiper les attaques possibles, les applications du schéma de tatouage doivent être étudiées en profondeur. Ces applications seront présentées au paragraphe suivant. En ce qui concerne la protection du copyright, on peut tenter de résumer ce chapitre par le tableau 1.3 proposant le cahier des charges idéal. On rajoutera qu'il est préférable que le schéma de détection soit semi-privé. On pourra alors automatiser les recherches d'images tatouées sur un réseau.

TAB. 1.3 – Cahier des charges idéal

Taille de I	$> 256 \times 256$
Qualité	5 ou > 35 dB
Longueur de marque	> 32 bits
Robustesse	maximum
P_{fp}	0
P_{fn}	minimum
Taille de K	o(Taille de I)

1.5 Les autres applications du tatouage

Les applications du tatouage numérique sont nombreuses ; leur diversité fait que les contraintes qu'elles imposent varient selon l'application envisagée. Les contradictions existant entre ces contraintes rendent impossible la création d'un algorithme universel adaptable à toutes les applications.

Il paraît donc nécessaire que la première étape de la conception d'un algorithme de tatouage comprenne la définition des applications auxquelles la méthode sera destinée puisque celles-ci définiront les besoins de la marque. La littérature relative au tatouage décrit abondamment les utilisations possibles du marquage [11] [1] [13] : on distingue généralement la protection de la propriété individuelle (détaillée auparavant), le suivi de document, la prévention de la redistribution non autorisée, la protection des droits de copie, l'indexation, l'information sur le support et l'intégrité du contenu du document.

L'intégrité de données multimédia

La marque permet de s'assurer que le contenu du document est authentique : il s'agit d'une marque *fragile*, qui subit des distorsions si le document a été altéré. Le concept de robustesse est ici différent : à l'inverse des autres applications du tatouage, la marque est conçue de manière à se détériorer dès que le document est modifié. Seules les modifications agressives doivent être prises en compte : la marque idéale en terme d'intégrité n'est pas affectée par des opérations de compression ou par l'ajout de bruit

inhérent à la transmission des données. Un exemple d'utilisation est l'authentification de conversations téléphoniques ou de vidéos afin de permettre leur utilisation lors de procès : la marque montrerait si le signal a subi des coupes, ou même les localiserait, permettant de vérifier si le sens premier de la conversation a été respecté.

Prévention de la redistribution non autorisée

L'objectif est de détecter les possesseurs licites d'un document qui sont à l'origine de sa distribution illicite. Les exemples les plus courants de telles distributions sont les copies (gravées) de CD audio, ou encore la mise à disposition de fichier audio au format mp3 sur les pages web personnelles. Une solution au problème de la redistribution non autorisée consiste à identifier séparément les acheteurs, en leur attribuant un numéro de série personnel.

La principale difficulté de conception d'un tel algorithme est qu'il faut générer autant de clefs qu'il existe d'acheteurs sans pour autant diminuer la robustesse du système. L'étude de la prévention de la redistribution non autorisée est donc indissociable des attaques de collusion (voir le paragraphe 1.4.2).

Un exemple concret d'application est le «paiement à la séance» sur les chaînes numériques et Internet. L'acheteur peut avoir l'intention de copier le document (film ou musique) pendant sa lecture pour le mettre ensuite à disposition sur sa page personnelle par exemple. Savoir que le document est tatoué d'un numéro de série unique permettant aux possesseurs des droits de remonter jusqu'à lui pourra éventuellement le dissuader de le pirater.

La réglementation des copies de données multimédia

Le cryptage d'un document ne suffit pas à assurer la protection de la copie : la sécurité est assurée le long du canal de transmission qui relie le vendeur à l'acheteur sous certaines hypothèse de robustesse ; mais une fois décrypté, le document n'est plus protégé et rien n'empêche le client de le copier. Le tatouage peut s'appliquer à cette famille de problèmes. Des informations relatives à la copie et à l'utilisation sont encodées dans la marque : il peut s'agir d'autorisations du type «pas de copies», «une seule copie», «plus de copies disponibles», ou encore «copie sans restriction». Le dispositif chargé de la lecture et/ou de la copie interroge le support en refusant de le lire ou de le copier si les données encodées ne le permettent pas. Ce dispositif suppose la construction d'une nouvelle génération de lecteurs audio. Les lecteurs DVD de seconde génération (permettant de graver des données vidéo) devraient être équipés d'un tel système de tatouage.

Information sur le support

La marque peut contenir des données publiques informatives sur l'oeuvre, de type *auteur, titre, date, adresse électronique* etc. Dans l'éventualité (très probable) où cette application interviendrait en complément d'une protection de la propriété, il s'agirait non pas d'une seconde marque, mais d'informations supplémentaires insérées dans la

première marque. On peut aussi envisager l'insertion d'une seconde marque entièrement publique, ce qui autoriserait le client à supprimer ces informations supplémentaires pour minimiser la taille des données stockées. Cette technique à été développée par Digimarc sur les images numériques [14] qui sont alors appelées «smart images». Ces images contiennent des adresses de pages Internet permettant d'obtenir des renseignements de nature publicitaire sur l'image.

Indexation

On peut envisager l'utilisation du tatouage afin de faciliter l'accès à des banques de données. La marque n'a pas besoin d'être robuste à de nombreux types d'attaque, puisqu'il ne s'agit plus de protection mais d'identification.

Suivi de document

La plupart des techniques définies ci-dessus peuvent être associées à des techniques de suivi de document. Un robot traqueur, appelé *bot*[3], explore un réseau donné à la recherche de données portant une certaine marque de propriété. Cette application privilégie très nettement des algorithmes rapides, qui font appel au minimum de données possible, comme les algorithmes aveugles.

Marquage visible

Pour certaines applications, l'implémentation d'une watermarque visible peut être envisagée. C'est par exemple le petit logo en bas à droite des images de journaux télévisé. Cette marque sert d'information aux consommateurs mais aussi d'argument dissuasif. Craver *et al.* [4] ont utilisé cette méthode pour la protection d'images digitales en introduisant un logo translucide qui recouvre toute l'image sans pour autant gêner sa compréhension. Les avantages de cette méthode sont la facilité d'implémentation et de détection de la marque, les inconvénients sont évidemment une plus grande fragilité du marquage aux attaques. Il est en effet très facile de couper la partie marquée de l'image où de supprimer la marque en reconstruisant l'image par interpolation. De plus, cette solution ne convient pas par exemple pour la vente d'images hautes qualités, et devient ridicule si l'on travaille sur des signaux sonores.

Conclusion

Certaines de ces applications pourraient à terme être utilisées dans le même protocole. Certains auteurs définissent ainsi un marquage à plusieurs niveaux : au premier niveau le secret porte sur l'existence d'une marque, le second sur la marque elle même [13], ainsi le fait que la donnée soit marquée peut être accessible à tous alors que le propriétaire reste inconnu.

[3]bot est le diminutif usuel de robot : programme informatique qui fonctionne automatiquement, sans l'intervention de l'homme. On distingue deux catégories de bots : les *agents* et les *araignées* (*spiders* ou *webcrawlers*). Ces définitions sont disponibles à l'url suivante : http ://webomedia.internet.com

1.6 Conclusion

Ce chapitre a introduit les principes du tatouage des données multimédia. Cette nouvelle discipline, au champ d'application très large, consiste à créer et à étudier des processus de stéganographie permettant d'introduire dans un support numérique une marque puis de la détecter. Parmi les applications possibles, nous avons détaillé celle concernant la protection du copyright. Les contraintes imposées au schéma de tatouage découlent directement du caractère applicatif de la discipline. Pour la protection du copyright, ces contraintes peuvent se résumer en termes d'imperceptibilité du marquage et de robustesse aux attaques. Nous nous sommes appuyés sur ces considérations pour proposer un cahier des charges idéal. En ce qui concerne la conception d'un schéma de tatouage nous avons insisté sur l'importance de l'étape de détection qui s'avère la plus fragile aux attaques.

Dans le chapitre suivant, nous étudierons les réponses données actuellement aux exigences imposées à un schéma de tatouage. Nous verrons que ce domaine de recherche est bouillonnant et propose des méthodes très diverses pour la création d'algorithmes de tatouage. Ces méthodes utilisent par exemple des critère psychovisuels, des domaines transformés de l'image, ou bien, des outils utilisés en théorie de la communication.

Chapitre 2

Les méthodes de tatouage existantes

Dés 1990, Tanaka *et al* [15] introduisent l'idée de «taguer» les images digitales pour cacher secrètement des informations et assurer ainsi les droits de propriété. Cependant les techniques de marquage prennent réellement leur essor en 1993, avec les méthodes de Caronni[16] et Tirkel [17]. En particulier, l'expression «digital watermark», sa définition ainsi que les diverses applications du tatouage sont mentionnées pour la première fois dans la seconde publication de Tirkel *et al.* intitulée *A Digital Watermark* [18]. C'est à partir des années 1995/1996 que l'intérêt des chercheurs et des industriels a considérablement augmenté. Le nombre de publications sur ce sujet passe de 2 en 93 à 103 en 1998 [1].

L'objectif de ce chapitre est de présenter un éventail représentatif des méthodes de tatouage et des différents schémas existants. Dans la plupart des présentations générales, les différentes méthodes sont classées selon le domaine dans lequel les transformations sont faites. P. Bas [19], les différencie selon la façon dont la marque est inscrite dans l'image : il distingue deux grands ensembles de méthodes, les additives et les substitutives. Nous choisissons cette classification mais préférons parler de méthodes «virtuelles» pour la dernière classe de schémas.

2.1 Méthodes additives

Les méthodes additives sont les plus nombreuses et consistent principalement à ajouter un «bruit» à l'image. La figure 2.1 montre le schéma complet d'une méthode additive. La première étape est la génération d'une marque W_0 qui est composée d'un bruit blanc modulant parfois un message M. La seconde étape est la pondération de cette marque grâce à la prise en compte de critères psychovisuels et de caractéristiques propres à l'image. La troisième étape est l'addition de la marque dans les valeurs de l'image. Cette incrustation peut se faire directement sur l'image (dans le domaine spatial) ou dans un domaine transformé. Cette section nous permettra de donner un aperçu de ces différentes étapes à travers des exemples de schéma de tatouage.

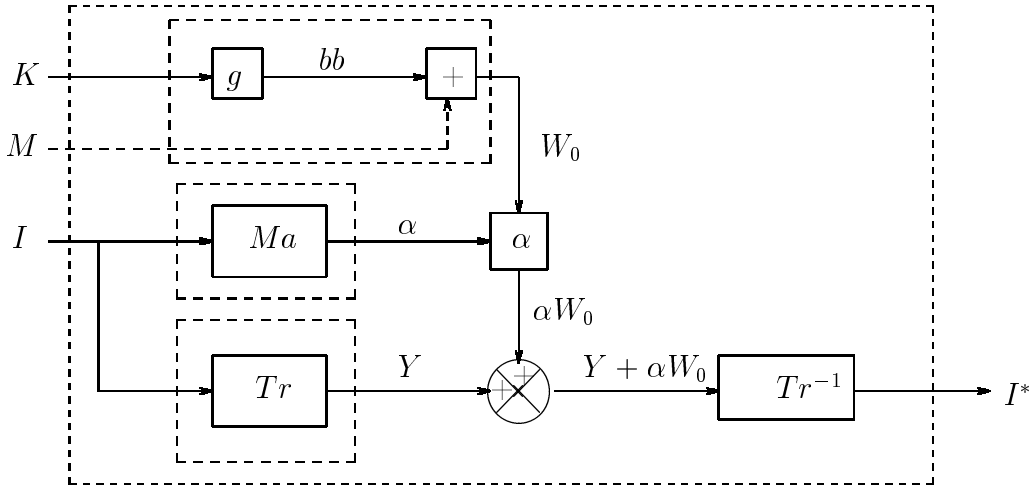


FIG. 2.1 – Schéma d'une méthode additive. La marque W_0 est construite en modulant le message M par un bruit blanc bb de générateur K. W_0 est ensuite pondéré par un gain α, issu du calcul d'un masque Ma psychovisuel. Cette marque est ajoutée à l'image ou à une transformée Tr de celle-ci.

2.1.1 Ajouter du bruit à l'image

Nous allons présenter ici les principes de deux méthodes classiques en tatouage d'images dont le principe général est d'ajouter un bruit sur l'image. La première méthode, plus ancienne, a été fondée sur l'idée d'ajouter des «patchs» à certains endroits secrets de l'image. La détection est basée sur la connaissance de ce secret. Dans la seconde méthode, un bruit large bande est ajouté à l'image, cette méthode est dérivée de techniques utilisées en théorie de la télécommunication. Après une présentation de ces deux méthodes, nous montrerons qu'on peut les considérer comme une unique méthode.

La méthode du *Patchwork*

Cette méthode, très classique, est introduite par Bender *et al* [20]. Elle est classée dans les méthodes à schéma semi-privé. Voici son principe :

A l'implémentation, l'algorithme sélectionne pseudo-aléatoirement (avec une clef K) N paires de pixels de l'image. Les valeurs des luminances de ces paires de pixels $(a_i, b_i)_{i=[1..N]}$ sont alors modifiées selon les formules suivantes :

$$a_i^* = a_i + 1 \tag{2.1}$$
$$b_i^* = b_i - 1 \tag{2.2}$$

On augmente de 1 la valeur d'un certain groupe A de pixels et on diminue d'autant un autre groupe B de même cardinal, la connaissance de ces deux ensembles étant conditionnée par celle de K.

A la détection, la somme S, différence entre les valeurs de ces deux groupes de pixels,

est calculée :

$$S^* = \sum_{i=1}^{N} (a_i^* - b_i^*) \tag{2.3}$$

Si l'on connaît la clef définissant les deux ensembles A et B et en supposant que l'image satisfait certaines propriétés statistiques, la valeur attendue de la somme est $2N$.

Si l'on ne connaît pas cette clef, on ne peut pas retrouver les deux ensembles, on ne peut que générer deux ensembles différents. Si ces ensemble sont générés pseudo-aléatoirement (avec une autre clef K'), l'espérance de la somme est alors nulle.

Ce principe de détection est fondé sur le résultat statistique suivant : si l'on choisit pseudo-aléatoirement deux ensembles de pixels de même cardinal, l'espérance de la somme de leur différence est nulle : $E(S) = \sum_{i=1}^{N} [E(a_i) - E(b_i)] = 0$ où E est l'espérance mathématique. Les deux sous-ensembles sélectionnés par les clefs doivent être grands et bien repartis dans l'image pour que cette propriété soit vérifiée.

On peut remarquer que l'implantation de la marque peut se résumer à l'addition de l'image avec une matrice W, de même taille que l'image et contenant la valeur 1 pour les pixels de l'ensemble A, -1 pour les pixels de B, 0 sinon. Si I est l'image originale, I^* l'image tatouée, on obtient :

$$I^* = I + W \tag{2.4}$$

où W est une matrice pseudo-aléatoire obtenue à partir de la clef K.

Cette technique, détaillée par Pitas *et al.* [21] fait partie des techniques dites à 1 bit d'insertion. C'est la connaissance de la clef qui identifie le propriétaire. Pour transmettre réellement un message par cette méthode, Langelaar *et al.* [22] l'appliquent successivement sur plusieurs blocs de l'image.

La méthode de l'étalement de spectre

On peut voir le problème de tatouage comme un problème de communication. Si l'on se réfère à la définition 1 du paragraphe 1.1, le tatouage consiste à transmettre un message (la marque) dans un environnement bruité. Dans cette modélisation, on considère l'image hôte comme un canal de transmission, la marque comme un message à transmettre et les attaques comme du bruit. Les outils utilisés en télécommunication s'imposent donc d'eux même.

Une des techniques utilisées largement en télécommunication est l'étalement de spectre[1]. Son principe est d'étaler le spectre d'un message afin de se servir de toute la bande passante du canal. Le message ainsi étalé sera donc présent sur toutes les fréquences et sera plus résistant aux altérations de cette bande. De plus, le message ressemble alors à un bruit blanc et donc très difficile à intercepter par un utilisateur non autorisé. On peut remarquer que la définition de ce principe inclut beaucoup de contraintes imposées au tatouage (présence de la marque sur tout le spectre fréquentiel, difficulté pour un utilisateur non-autorisé de le détecter).

[1] Cette technique qui date des années 40 a d'abord été utilisée pour des applications militaires et est très utilisée aujourd'hui en télécommunication, par exemple pour les téléphones cellulaires, le GPS (Global Positioning Satellite) et le VSATS (Very Small Aperture Satellite Terminals).

L'étalement du spectre du message est classiquement effectué en modulant la donnée par une séquence pseudo-aléatoire de fréquence bien supérieure. On peut formaliser cette technique ainsi : soit m, le message que l'on veut transmettre, bb la séquence pseudo-aléatoire, le signal résultant W_0 est donnée par :

$$W_0 = (\uparrow R)m \oplus bb \tag{2.5}$$

où R est la fréquence de ré-échantillonnage, $\oplus$ le «ou exclusif», $\uparrow$ l'opérateur de ré-échantillonnage. Une fois cet étalement de spectre opéré, la matrice W_0 est ajoutée à l'image avec une force α, l'image résultante I' est donnée par l'équation :

$$I^* = I + \alpha W_0 \tag{2.6}$$

Si on a accès à l'image originale, la détection extrait W_0 puis m, bb étant connu. Si le détecteur est semi-privé, la détection fonctionne par corrélation avec :

$$C = \frac{< I^*, bb >}{||bb||^2} = \frac{< I, bb > + \alpha < W_0, bb >}{||bb||^2} \tag{2.7}$$

Si l'image originale et le bruit blanc sont indépendants et que ce bruit est centré, alors $E(< I, bb >) = 0$, on retrouve le message m.

La particularité de ces méthodes réside dans l'emploi du pseudo-bruit permettant d'étaler le spectre du message. Même si toutes les séquences aléatoires peuvent à priori convenir, certaines (m-séquences, codes de Gold) possèdent des propriétés d'autocorrélation permettant une meilleure réception du message et une minimisation des interférences. Ces séquences sont utilisées en CDMA (Code Division Multiple Access) où plusieurs utilisateurs peuvent coexister sur la même bande passante si chaque utilisateur est assigné à une séquence distincte.

La séquence pseudo-aléatoire est le secret de l'algorithme, elle est générée par la clef K qui sera stockée. Pour assurer la sûreté du système, il faut que la taille de cette séquence soit assez grande. C'est pour cela que la plupart des algorithmes utilisant cette méthode transmettent un message à un bit $m = 1$.

Tirkel *et al.* [17] [18] ont été les premiers à utiliser la technique de l'étalement de spectre pour le tatouage. Cette méthode est maintenant utilisée dans la grande majorité des schémas de tatouage additifs.

Conclusion

P. Bas [19] démontre que les méthodes de patchwork et celles utilisant l'étalement de spectre fonctionnent selon le même principe. Nous avons vu que l'étape d'insertion de la méthode du Patchwork était en effet équivalente à un ajout de bruit sur l'image originale (voir l'équation 2.4). Nous allons maintenant nous intéresser à la corrélation. Soit la matrice de bruit W comme définie pour l'équation 2.4. Prenons cette matrice normée, on a alors :

$$C =< I^*, W >= \sum_{W_i=1} I^*(i) - \sum_{W_i=-1} I^*(i) = S^* \tag{2.8}$$

Cette égalité montre la similitude entre les deux méthodes.

Les techniques présentées ci-dessus sont initialement conçues pour des applications de télécommunication. Elles ne prennent donc pas en compte toutes les contraintes nécessaires à un tatouage. En particulier, l'imperceptibilité du tatouage n'est pas prise en compte. Nous présenterons dans le paragraphe 2.1.3 les solutions envisagées pour introduire cette contrainte dans l'algorithme.

La robustesse de ce type de méthode varie selon l'attaque envisagée. En général, ces méthodes donnent d'assez bons résultats sauf pour les attaques de désynchronisation du signal (voir le paragraphe 1.4.2). Un moyen d'augmenter la robustesse du schéma aux attaques est de tatouer l'image dans des domaines transformés. Le paragraphe suivant présente certains schémas utilisant les domaines transformés de l'image.

2.1.2 Utilisation de domaines transformés

Les algorithmes de tatouages additifs peuvent fonctionner dans n'importe quel domaine transformé de l'image, à condition que la transformation soit inversible. Le domaine le plus utilisé est le domaine spatial car il permet l'implémentation la plus facile et nécessite l'algorithme le moins coûteux en temps de calcul. Il est utilisé pour les applications temps réel et permet d'utiliser les critères du SVH [23] [24] [25] [26] [27]. L'utilisation du domaine fréquentiel [9] [28] [29] [30] [31] (obtenu après une DFT[2] ou DCT[3]) ne nécessite pas trop de temps de calculs grâce aux algorithmes de transformations rapides. L'utilisation de la DCT permet une bonne robustesse du schéma de tatouage à la très populaire compression JPEG [32] qui utilise cette transformée. L'utilisation de la DWT[4] [33] [29] [34] [35] est intéressante car cette transformée est utilisée dans les nouveaux formats de compression comme JPEG2000. De plus, cette transformée peut être interprétée comme la décomposition de l'image en sous bandes fréquentielles et est donc souvent proche d'une décomposition en canaux perceptifs.

Dans cette section, nous allons présenter quelques exemples de schémas de tatouage utilisant des domaines transformés.

Dans la transformée en cosinus discrète (DCT)

Cox *et al.* [9] présentent une méthode de tatouage à étalement de spectre dans les coefficients DCT de l'image. Leur principale motivation est de tatouer les composantes perceptuellement significatives de l'image (celles qui sont nécessaires à la compréhension de celle-ci). Un bruit blanc W gaussien de générateur la clef secrète K, modifie les n coefficients DCT v_i de plus grandes amplitudes (exceptée la composante continue) par

[2]transformée de Fourier discrète
[3]transformée en cosinus discrète
[4]transformée en ondelettes discrète

l'une des relations suivantes :

$$v_i^* = v_i + \alpha w_i \tag{2.9}$$
$$v_i^* = v_i(1 + \alpha w_i) \tag{2.10}$$
$$v_i^* = v_i e^{\alpha w_i} \tag{2.11}$$

La présence de la watermarque est vérifiée par corrélation après extraction de la marque. Cette méthode est très robuste et donne de bons résultats face aux attaques de type changement d'échelle, compression JPEG, passage à l'analogique puis au numérique, et attaque par collusion. Le principal désavantage de cette méthode est que l'image originale doit être connue pour permettre l'extraction de la marque.

Dans la transformée en ondelette discrète

Kundur *et al.*[34], appliquent un schéma de tatouage additif dans le domaine de la transformée en ondelettes discrète de l'image. La marque, une matrice binaire dans $\{-1, 1\}$, est décomposée en quatre sous-marques par DWT au niveau 1. L'image est décomposée en ondelettes jusqu'à un niveau L (en pratique $L = 4$). Les coefficients de détails de tous les niveaux sont alors modifiés : on y ajoute les sous marques pondérées par un seuil psychovisuel adaptatif. L'image marquée est alors reconstruite par transformation inverse. La détection se fait avec l'image originale, on extrait les valeurs de la marque à chaque résolution, la marque extraite finale étant la moyenne des valeurs obtenues. Cette méthode est très robuste à la compression et à l'ajout de bruit blanc mais reste sensible au filtrage.

Barni *et al.* [36] proposent un schéma de tatouage fondé sur le même principe, mais à détection semi-privée : la watermarque (un bruit blanc) est ajoutée adaptativement dans chacunes des trois sous-bandes de détails du niveau 1 de la décomposition en ondelettes. Du fait de la redondance de la marque (elle est insérée trois fois dans l'image), ce schéma donne de bonnes performances de détection.

Dans la transformée Fourrier-Mellin

Le problème de synchronisation de la marque peut être résolu en choisissant un domaine transformé de l'image invariant par translation, rotation et changement d'échelles, comme le proposent Ó Ruanaidh *et al.* dans [30]. La figure 2.2 présente le schéma de tatouage contenant les étapes de transformations de l'image du domaine spatial jusqu'au domaine invariant. Cette transformation est composée d'une transformée de Fourier suivie d'une transformée de Fourier-Mellin. Pour que la transformation soit inversible, les signaux de phases de l'image originale sont conservés et ré-utilisés lors du retour au domaine spatial.

L'invariance par translation est obtenue par la transformation de Fourier de l'image dont on ne prend que le module. Les invariances par rotation et changement d'échelles sont obtenues par transformation de Fourier-Mellin du module. En effet, cette transformation peut être vue comme la composée d'un changement de base en log-polaire et

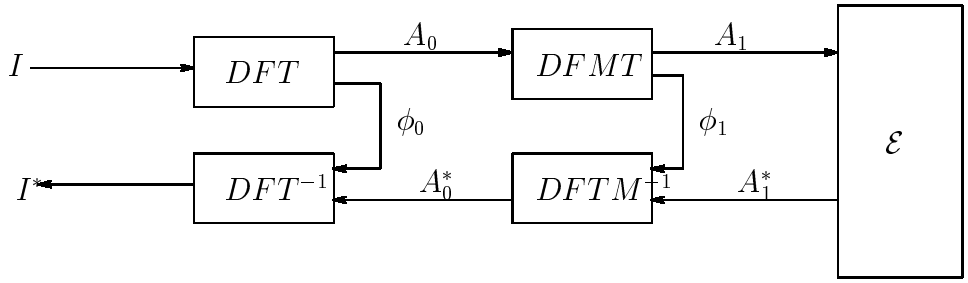


FIG. 2.2 – Schéma du tatouage dans le domaine d'invariance. La DFT est la transformée de Fourier discrète, la $DFMT$ celle de Fourier-Mellin. Les signaux A_i représentent les amplitudes, ϕ_i les phases des transformées de l'image.

d'une transformée de Fourier. Le changement de base a la propriété de transformer les rotations et changement d'échelles en translation, la transformé de Fourier, dont on ne prend que le module, rendant le tout invariant.

L'insertion et la détection de la marque se font de façon classique dans le domaine transformé de l'image.

Dans la transformée en ondelettes complexes

Dans [35], Loo et Kingsbury choisissent eux aussi d'appliquer les méthodes à étalement de spectre dans un domaine invariant par translation. Pour cela, ils utilisent une décomposition en ondelettes complexes. Pour des raisons de meilleure reconstruction, le calcul de l'arbre de décomposition à valeur complexe se fait par l'intermédiaire de deux arbres, l'un représentant la partie imaginaire, l'autre la partie réelle des coefficients en ondelettes.

Dans les canaux perceptuels

Saadane *et al.* [37] utilisent un modèle psychovisuel pour définir des sites préférentiels à l'insertion de la marque. La modélisation du SVH est obtenue en décomposant le spectre de l'image (obtenu après transformation de Fourier) en différentes sous-bandes, et en appliquant ensuite une sélectivité angulaire. Le modèle multi-canal est présenté sur la figure 2.3. Nous détaillons cette Décomposition en Canaux Perceptuels (DCP) car nous nous servirons de cette approche au chapitre 11. La figure 2.3 représente la partition de l'espace des fréquences obtenue par la modélisation.

L'espace des fréquences est divisé en 17 sous bandes distinctes de la manière suivante : Cinq bandes radiales appelées couronnes sont sélectionnées. La couronne I représente les basses fréquences, la V-ième représente les hautes fréquences. Ces couronnes sont ensuite décomposées en sous bandes d'orientations distinctes. Les deux premières couronnes ne sont pas décomposées. La troisième est décomposé en 4 orientations différentes et les dernières couronnes en 6 orientations.

Dans le but d'obtenir le meilleur compromis robustesse/invisibilité du tatouage, les

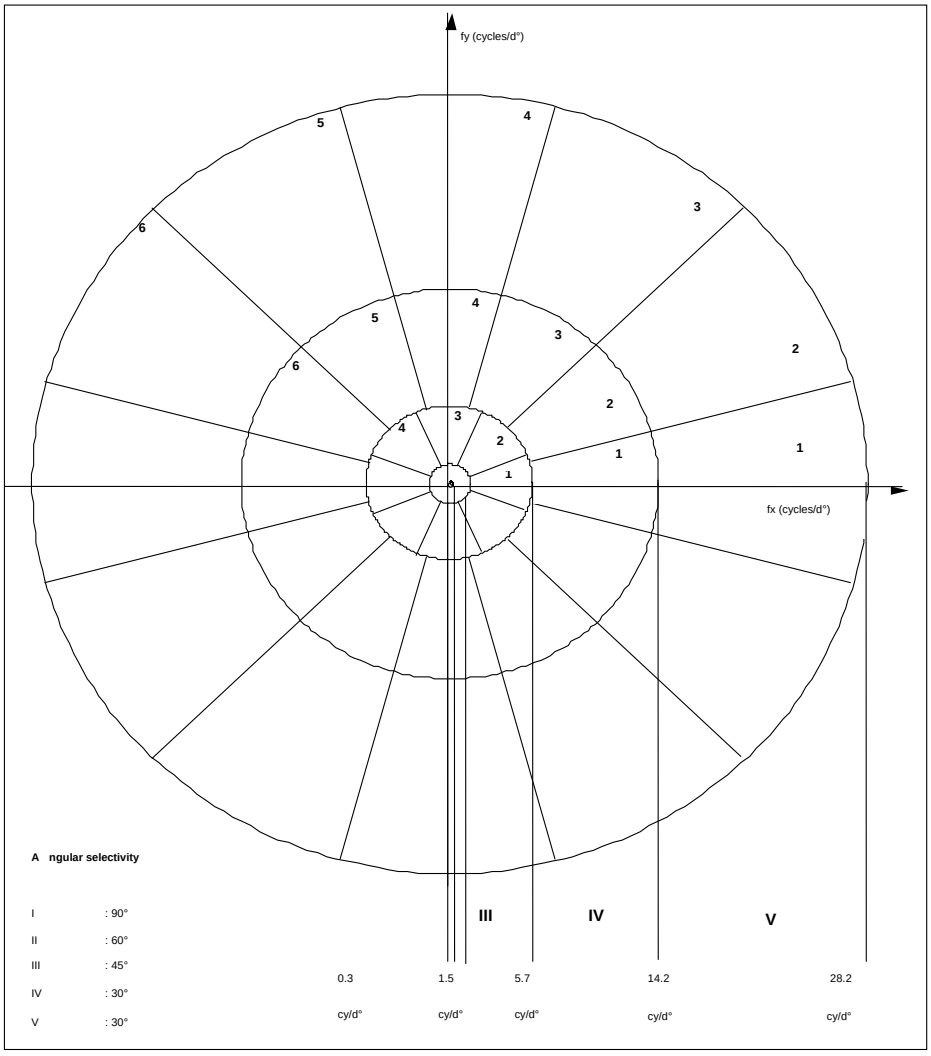


FIG. 2.3 – Décomposition en canaux perceptuels

auteurs ont choisis d'utiliser les sous-bandes (IV,3) et (V,4) [37] pour insérer la marque. La marque est un code binaire qui est ajouté (adaptativement) sur chaque sous-bande. L'image ainsi tatouée est reconstruite.

2.1.3 Modulation du bruit selon l'image

Dans les méthodes présentées ci-dessus le bruit est ajouté uniformément à la valeur des pixels de l'image. La contrainte d'invisibilité n'est pas considérée sauf dans le cas de la DCP vue ci-dessus. L'idée permettant de remédier à ce manquement au cahier des charges est de pondérer l'insertion du bruit par une matrice dépendant des caractéristiques de l'image et de considérations psychovisuelles. L'amplitude du bruit sera augmentée dans les zones où l'image est très texturée, elle sera diminuée dans les zones très uniformes. Ainsi, l'utilisation de modèles psychovisuels en tatouage d'images permet de répondre à deux contraintes :

- L'algorithme garantit l'invisibilité du marquage
- Le compromis invisibilité-robustesse est optimisé

Le principe est de maximiser la force de tatouage α pour chaque pixel selon les caractéristiques de l'image et des critères psychovisuels. L'implémentation de la marque est alors donnée par la relation 2.12, la détection ne change pas.

$$\forall (i,j) \in [1..N]^2 \quad I^*(i,j) = I(i,j) + \alpha_I(i,j)W(i,j) \tag{2.12}$$

Le calcul de la matrice des forces de tatouage α_I est fondé sur une particularité du système visuel humain (SVH) appelée effet de *masquage*. Le masquage a lieu lorsqu'un signal (la marque) est rendu imperceptible par la présence d'un autre signal dit *masquant* (l'image). Plusieurs modèles de masque ont été utilisés en tatouage d'image, certains modèles sont dans le domaine spatial [38] [39], d'autres dans le domaine fréquentiel [40], [37]. F. Autrusseau *et al.* ont proposé un masque permettant d'allier des caractéristiques fréquentielles du SVH et des caractéristiques spatiales de l'image traité. La méthode d'obtention de ce masque est donnée dans [37]. Des exemples de masques seront donnés au chapitre 11.

2.2 Méthodes virtuelles

Nous appelons tatouage *virtuel*, un tatouage où la marque n'est pas ajoutée sur les données mais où la marque impose des contraintes aux valeurs de l'image. Ces méthodes de tatouages ne sont pas additives : l'information n'est pas ajoutée à l'image, ni substitutives : l'information ne remplace pas des valeurs de l'image.

Considérons un exemple simple pour illustrer cette définition :

- la clef secrète K détermine un ensemble de N paires de pixels $(a_i, b_i)_{i=[1..N]}$.
- La watermarque W, de longueur N est exprimée en modifiant la relation d'ordre liant les pixels entre eux. Soit (a_i^*, b_i^*) les pixels modifiés.

$$\text{- si } W_i = 1 \text{ et si } \begin{array}{ll} a_i \leq b_i & a_i^* = a_i \text{ et } b_i^* = b_i \\ a_i > b_i & a_i^* \text{ et } b_i^* \text{ sont choisis tels que } a_i^* \leq b_i^*. \end{array}$$

$$\text{- si } W_i = -1 \text{ et si } \begin{array}{ll} a_i \leq b_i & a_i^* \text{ et } b_i^* \text{ sont choisis tels que } a_i^* > b_i^* \\ a_i > b_i & a_i^* = a_i \text{ et } b_i^* = b_i. \end{array}$$

– Les pixels modifiés sont réintégrés à leurs places dans l'image

La détection consiste à lire le message en regardant comment les paires de pixels (trouvées grâce à K) sont ordonnées.

Au travers de cet exemple très simple apparaissent les avantages d'utiliser ce type de méthode. D'une part, on peut transmettre une marque de longueur non négligeable. D'autre part, l'image n'est plus ici considérée comme un canal bruité pouvant créer des interférences avec la marque mais comme le support du marquage. En outre, on a une grande liberté sur la façon de modifier les composantes. Dans notre exemple, ces composantes ne seront pas toujours modifiées (une fois sur quatre pour une marque centrée) et on peut le faire de multiples façons : ajouter un coefficient, multiplier par un autre... Ces algorithmes ne sont jamais inversibles, l'information initiale étant perdue. Ainsi, les attaques malignes ne consisteront pas à enlever la marque (on ne peut pas enlever de relation d'ordre) mais à la brouiller (l'attaquant inversera la relation). Chen *et al.* [3] ont présenté une étude de ce dernier type d'attaque et ont quantifié la dégradation nécessaire au brouillage de la marque. Une étude similaire sera proposée au paragraphe 13.2.

Plus généralement les schémas de tatouage virtuels peuvent être décrits par les étapes présentées ci-dessous :

– La clef privée K sélectionne des composantes de l'image. Elles peuvent être des pixels, des coefficients issus de domaines transformés ou encore des propriétés de l'image.

– La watermarque W est exprimée en modifiant les caractéristiques des composantes pointées par K. Cela peut être une relation d'ordre, un critère de similarité, une propriété géométrique de l'image ou encore l'appartenance à un certain espace fonctionnel.

– Ces composantes sont ensuite réintégrées dans l'image

Comme on l'a vu dans l'exemple, la détection consiste à récupérer les composantes secrètes et à examiner leurs caractéristiques. On peut parler ici de lecture de la marque.

Dans les paragraphes suivants, nous présenterons des exemples de méthodes de tatouage virtuels.

2.2.1 Utilisation de la compression JPEG

Le premier processus de tatouage par modification des coefficients DCT d'une image est présenté par Zhao and Koch [28]. Le principe est de calquer la méthode de compression

JPEG, qui utilise cette transformée. La méthode sera alors robuste à cette transformée très répandue.

- L'image est décomposée en blocs de 8×8 pixels, dont certains sont choisis par la clef K pour porter le message.
- Les blocs sont ensuite transformés par DCT, puis les modifications se font sur un triplet (déterminé lui aussi par la clef) de coefficients basses fréquences (C_1, C_2, C_3). Par souci d'invisibilité, on ne modifiera jamais les trois coefficients des plus basses fréquences. Le triplet modifié doit respecter des contraintes d'ordre différentes selon que la marque à implanter W porte le bit 0 ou 1 :

$$C_1 > C_3 + Cte \quad \text{et} \quad C_2 > C_3 + Cte \quad \text{si} \quad w_i = 1 \tag{2.13}$$
$$C_1 + Cte < C_3 \quad \text{et} \quad C_2 + Cte < C_3 \quad \text{si} \quad w_i = 0 \tag{2.14}$$

  Pour améliorer la robustesse, la modification se fait sur les valeurs quantifiées du triplet. Elle consiste à augmenter/diminuer les valeurs des coefficients en minimisant les distorsions (on utilise comme mesure les moindres carrés).

L'insertion n'est possible que si la différence entre les composantes pointées n'est pas trop importante (ce qui est généralement le cas pour des images réelles). La détection consiste à la lecture de l'ordre des coefficients.

2.2.2 Utilisation de la compression fractale

En 1996, J. Puate *et al.* [41] présentent un schéma de tatouage basé sur une modification de l'algorithme de compression fractale. L'idée principale de cette technique de compression est d'exprimer une image par la donnée d'un ensemble d'applications affines contractantes.

IFS et définition d'une image

Rappel : Soit la donnée d'un IFS (Iterated Function System), c'est à dire la donnée d'un espace métrique $(\pounds, d)$ complet et d'un ensemble de transformations contractantes β_i définies sur $\pounds$. La transformation fractale associée est $\mathcal{B}(E) = \bigcup_{i=1}^{n} \beta_i(E)$ où E est un sous ensemble non vide compact de $\pounds$. On sait alors que $\mathcal{B}$ possède un unique point fixe A, appelé attracteur ($A = \mathcal{B}(A)$ et $\forall E, \quad \lim_{n\to\infty} \mathcal{B}(E)^n = A$).

Si on se place sur $\pounds$ l'espace des images, une image A qui est l'attracteur d'un IFS est entièrement définie par celui-ci et on la construit par itération de $\mathcal{B}$ sur n'importe quelle image initiale jusqu'à ce que les images obtenues ne varient plus significativement.

Principe de la compression

La compression fractale pose le problème inverse : connaissant une image quelconque, comment trouver des applications contractantes permettant de la définir, ou de définir une image très proche ? Le théorème du collage répond à cette question en bornant la distance entre un attracteur A et un ensemble M par la distance entre cet ensemble et

son image par l'application contractante. C'est à dire que M et A sont proches si M et $\mathcal{B}(M)$ le sont.

La méthode issue de cette théorie consiste tout d'abord à partitionner l'image en blocs M_i d'une part et en blocs m_i, de plus petite taille, d'autre part. Chaque bloc m_i sera approximé par le meilleur M_i ayant subi la meilleure application contractante (définissant alors les β_i). Le théorème du collage implique alors la convergence de l'IFS ainsi caractérisé vers une image proche de l'originale.

Tatouage

La méthode de tatouage par compression fractale consiste à contraindre la recherche des blocs M_i. L'algorithme peut se résumer comme ci-dessous :

- La clef K sélectionne N blocs m_i
- W est exprimée de façon suivante :
  - si $w_i = 0$, la recherche de M_i se fera dans un voisinage V_0 de m_i (c'est un carré entourant m_i)
  - si $w_i = 1$, la recherche de M_i s'effectuera dans un autre voisinage V_1 distinct de V_0 (c'est une couronne entourant V_0)
- Pour les blocs non sélectionnés par K, M_i est recherché dans l'union des deux voisinages
- L'attracteur de l'IFS ainsi défini est calculé, créant alors l'image marquée.

A la détection, il suffit de regarder les propriétés de l'IFS caractérisant l'image.

2.2.3 Utilisation de quantificateurs

Quantification Vectorielle Spatiale Dans [42], Chen *et al.* introduisent une méthode de tatouage à clef publique fondée sur le principe de codage par quantification vectorielle.

La quantification vectorielle consiste à remplacer des blocs de l'image par d'autres appartenant à un dictionnaire prédéfini (le choix des blocs minimise les distorsions infligées à l'image).

Dans le schéma de tatouage présenté ici, le nombre de dictionnaires est fonction de la quantité d'informations contenues dans la marque. Selon la valeur de la marque, un dictionnaire sera choisi. Dans chaque dictionnaire, la taille et la variété des blocs déterminent la distorsion produite par l'insertion de la marque.

La détection de la marque est accomplie en vérifiant que les blocs de l'image appartiennent bien au dictionnaire utilisé lors de l'insertion.

Une étude statistique sur les mesures de distorsions de l'image est présentée. Les auteurs insistent particulièrement sur le fait que le tatouage ne fournit pas de distorsions visibles (au sens des moindres carrés) et que l'on ne peut brouiller la marque qu'en dégradant plus fortement l'image. Une étude similaire est présentée paragraphe 13.2.

Dans les coefficients en ondelettes Dans [43], Kundur *et al.* appliquent une méthode substitutive au domaine défini dans [34]. La méthode peut se résumer ainsi :

- La transformée en ondelettes du signal est calculée jusqu'à un niveau l.
- A chaque résolution j (niveau de la décomposition en ondelettes), on choisit aléatoirement (avec la clef K) trois coefficients de détails appartenant à trois orientations fréquentielles distinctes (horizontales, verticales et diagonales). Ces coefficients sont d'abord classés selon leur valeur : $c^1 \leq c^2 \leq c^3$, puis le coefficient «médian» c^2 est modifié. Les modifications se font par quantification. On divise le segment $[c_1, c_3]$ en $2Q-1$ segments de longueur Δ (Q est la force du tatouage)
  - si $w_i = 1$, $c^{*2} = c^3 - p_3\Delta : c^2$ est quantifié sur une grille passant par c^3.
  - si $w_i = 0$, $c^{*2} = c^1 + p_1\Delta : c^2$ est quantifié sur une grille passant par c^1.

  Les coefficients entiers p_1 et p_3 minimisent les distorsions.

La détection s'effectue en regardant la position de la valeur moyenne du triplet par rapport aux deux autres. Cette technique a pour avantage de permettre de transmettre une marque de grande taille ($(N^2-1)/3$ pour une image de taille N^2), sa robustesse peut donc être fortement augmentée par redondance ou emploi de code correcteurs d'erreurs.

2.3 Conclusion

Nous avons présenté dans ce chapitre un aperçu des techniques utilisées actuellement en tatouage d'images digitales. Nous avons fait la distinction entre deux familles de méthodes : les schémas additifs et les schémas virtuels. Dans le premier ensemble de méthodes, l'algorithme d'implémentation ajoute un bruit sur l'image. Cette méthode dérive des techniques de communication et a donnée lieu à de nombreuses études. En particulier, un grand soin est apporté à l'optimisation du compromis robustesse-invisibilité par l'utilisation de critères psychovisuels.

Dans le deuxième type de méthodes, la marque impose une structure à l'image. Utiliser cette approche pour le tatouage d'images présente plusieurs avantages :

- Mathématiquement, les méthodes virtuelles peuvent souvent être considérées comme des *projections*. Elles sont donc par définition non-inversibles. Un pirate ne pourra pas enlever la marque, il ne pourra qu'espérer la brouiller.
- La marque exprime des contraintes sur l'image : les modifications induites par le marquage ne sont pas fixées. Cette liberté peut permettre d'optimiser le compromis robustesse-invisibilité.
- La clef et la marque sont indépendantes et de grandes tailles (en général de l'ordre de la taille des images).
- La détection est aveugle, elle consiste à lire la marque. Elle est toujours parfaite en l'absence d'attaque : l'image n'interfère pas avec la marque comme cela se produit pour le premier type de méthodes.

Les méthodes virtuelles semblent donc bien adaptées à notre problème, c'est une méthode de ce type que nous présenterons dans la suite de ce rapport.

Chapitre 3

Conclusion

Le tatouage pour la protection des données multimédia est un problème actuel et un domaine de recherche bouillonnant obéissant à des besoins urgents. Nous avons insisté pour considérer une approche globale du problème. Elle consiste en premier lieu à choisir le domaine applicatif et à en établir le cahier des charges. C'est ce que nous avons fait au premier chapitre en détaillant les contraintes et propriétés inhérentes à notre application : la protection des droits d'auteurs et du copyright.

Le deuxième chapitre a donné un aperçu des schémas de tatouage développés récemment. Nous avons choisis de distinguer les méthodes additives et virtuelles. Après avoir présenté ces méthodes, nous avons choisi de travailler sur le second type de techniques qui nous semble mieux adapté.

L'algorithme que nous allons présenter est donc fondé sur le principe des méthodes virtuelles : l'implémentation est une projection de l'espace des images. Cette projection est réalisée en déformant une structure de l'image. Notre but est donc de trouver une structure qui caractérise l'image. Cette structure doit pouvoir être contrainte sans dégradation visible sur l'image. Une fois les modifications produites, cette structure doit être assez robuste pour supporter un grand ensemble d'attaques sans être modifiée. Nous retrouvons ici le compromis invisibilité-robustesse.

La structure que nous avons choisi est une «meilleure» base de décomposition en paquets d'ondelettes. Dans le chapitre suivant nous introduirons des notions sur la transformée en ondelettes discrète et sa généralisation : la décomposition en paquets d'ondelettes. Nous donnerons ensuite des exemples d'algorithmes de sélection de bases de paquets d'ondelettes. Nous présenterons enfin l'algorithme qui permettra de choisir la base sur laquelle nous allons exprimer le tatouage.

Deuxième partie

Décomposition en paquets d'ondelettes et sélection de meilleure base de paquets d'ondelettes

Introduction

La *transformée en ondelettes* d'un signal permet de représenter le signal sur un espace bidimensionnel appelé le plan temps-échelle, fournissant sur le signal des informations conjointes en temps et en fréquence. Le pavage du plan temps-fréquence induit par cette transformée a pour particularité de permettre une résolution temporelle fine aux hautes fréquences et une résolution fréquentielle fine aux basses fréquences. Cette propriété permet souvent une analyse intéressante du signal mais reste rigide. La décomposition en paquets d'ondelettes est une extension de la transformée en ondelettes discrète permettant de choisir le pavage du plan temps-fréquence. Ce choix est réalisé à travers la sélection d'une base de paquets d'ondelettes. En général, la base est sélectionnée selon le signal traité et selon un critère répondant aux contraintes de l'application. Cette base sera appelée *meilleure base*.

Nous allons présenter dans cette partie les différents outils cités ci-dessus. Dans le premier chapitre, nous introduirons la transformée en ondelettes continue puis nous parlerons de la transformée en ondelettes discrète et de l'analyse multirésolution permettant de générer certaines de ces ondelettes. Dans le second chapitre, nous présenterons l'algorithme de décomposition en paquets d'ondelettes. Puis, nous donnerons des exemples de sélection de meilleure base. En particulier, nous présenterons le critère que nous utiliserons dans la méthode de tatouage proposée.

Dans cette partie, nous nous sommes volontairement limités aux notions nécessaires à la compréhension de la méthode décrite dans la suite du rapport. La bibliographie de ce chapitre est fondée sur [44] [45] [46] [47] [48] [49] [50].

Chapitre 4

La transformée en ondelettes discrète

La transformée en ondelettes discrète peut être vue comme issue de l'échantillonnage critique de la transformée en ondelettes continue. Certaines transformées peuvent être obtenues par analyse multirésolution (AMR). Dans ce chapitre, nous présenterons ces deux points de vues. Dans le premier cas, nous insisterons sur le pavage du plan temps-échelle induit par cette transformée. Afin de clarifier le propos, nous introduirons les notions utiles par l'intermédiaire de définitions sur la transformée de Fourier à court terme puis nous définirons la transformée en ondelettes continue. Dans le second cas, nous présenterons la théorie de l'AMR et l'algorithme pyramidal permettant d'obtenir les coefficients de la transformée en ondelettes discrète par filtrages et décimations successifs. Afin de simplifier les notations, nous considérerons dans un premier temps un signal à une dimension pour présenter les différentes notions sur les ondelettes puis nous généraliserons les propos au cas bidimensionel.

4.1 La transformée en ondelettes continue

4.1.1 Introduction : La transformée de Fourier à Court Terme

4.1.1.1 Définition

La transformée de Fourier est un outil permettant de connaître le comportement fréquentiel d'un signal. En utilisant cette transformation, on perd toute information relative au temps. Pour remédier à cela, et dans le cadre des signaux à énergie finie ($x(t) \in L^2(\mathbb{R})$), on utilise un outil «temps fréquence» : on restreint l'existence du signal autour d'une date t, grâce à une fenêtre d'analyse $g(u-t)$ centrée sur cette date, puis on en prend sa transformée de Fourier :

$$\int x(u)g(u-t)e^{-i2\pi\nu u}du \tag{4.1}$$

On fait alors glisser cette fenêtre le long du signal, ce qui permet d'en mesurer le contenu spectral au cours du temps. On appelle cette transformation la transformée de Fourier

à Court Terme, on la note STFT (Short Term Fourier Transform).

$$T_x(\nu,t) = \int x(u)g(u-t)e^{-i2\pi\nu u}du = \int x(u)g^*_{\nu,t}(u)du =< x(u), g_{\nu,t}(u) > \tag{4.2}$$

Cette transformation peut être vue comme la projection du signal sur des atomes temps fréquences, les $g_{\nu,t}$. Ces vecteurs sont obtenus par applications successives de deux opérateurs élémentaires à une fonction-mère de référence g. L'opérateur de translation temporelle déplace celle-ci le long de l'axe des temps, tandis que l'opérateur de translation (ou de modulation) fréquentiel la fait glisser le long de l'axe des fréquences. On obtient alors la définition suivante des atomes :

$$g_{\nu,\tau}(t) = g(t-\tau)e^{i2\pi\nu t} \tag{4.3}$$

4.1.1.2 Résolution dans le plan temps fréquence

La STFT ne contient pas plus d'information que la transformée de Fourier, elle fournit simplement une représentation du signal sur un espace bidimensionnel. $T_x(\nu,t)$ ne peut cependant pas décrire le contenu du signal strictement à l'instant t et à la fréquence ν car l'atome d'analyse $g_{\nu,\tau}$ est caractérisé par ses extensions conjointes temporelle Δt et fréquentielle $\Delta\nu$. Il y a donc mélange de l'information contenue dans le signal pour l'intervalle de temps $[t-\Delta t/2, t+\Delta t/2]$ dans la bande de fréquence $[\nu-\Delta\nu/2, \nu+\Delta\nu/2]$.

Une localisation temps-fréquence idéale, infiniment précise ($\Delta t = 0$ et $\Delta\nu = 0$) est interdite par le principe de Gabor-Eisenberg qui stipule que la résolution conjointe temps-fréquence est minorée[1] :

$$\Delta t\Delta\nu \geq \frac{1}{4\pi} \tag{4.4}$$

où

$$\Delta t^2 = \frac{\int t^2|g(t)|^2dt}{\int |g(t)|^2dt} \quad \text{et} \quad \Delta\nu^2 = \frac{\int \nu^2|G(\nu)|^2d\nu}{\int |G(\nu)|^2d\nu} \tag{4.5}$$

G étant la transformée de Fourier de la fenêtre d'analyse g.
Cette relation confère aux $g_{\nu,t}$ le statut d'atomes, portant une portion irréductible d'information temps-fréquence.
De plus, les résolutions temporelles et fréquentielles ne sont pas modifiées par les opérateurs de translation en temps et en fréquence et restent égales à celles de la fonction mère :

$$\begin{cases} \Delta t_{g_{\nu,t}} = \Delta t_g \\ \Delta t_{g_{\nu,t}} = \Delta t_g \end{cases} \tag{4.6}$$

Une représentation dans le plan temps-fréquence, conduit à un pavage en cellules élémentaires, dont la forme ne varie ni avec le temps, ni avec la fréquence, il est représenté figure 4.1.

[1] On a égalité pour les fonctions à enveloppe gaussienne

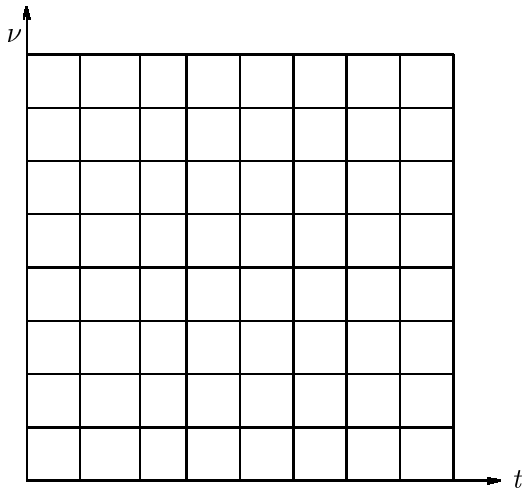


FIG. 4.1 – Pavage du plan temps-fréquence

Remarque : Le choix d'une fenêtre longue conduit à une bonne résolution en fréquence, mais à une résolution temporelle assez mauvaise. De même, une fenêtre courte privilégie la résolution temporelle au détriment de la résolution fréquentielle.
Comme la transformée de Fourier, la STFT préserve l'énergie :

$$E_x = \int \int |T_x(\nu, t)|^2 d\nu dt \tag{4.7}$$

De plus, on peut reconstruire le signal :

$$x(t) = \int \int T_x(\nu, t) g_{\nu,\tau} dt d\nu \tag{4.8}$$

si $g(t)$ est d'énergie unité.

4.1.1.3 Conclusion

La STFT ne représente pas l'ensemble des représentations temps-fréquence mais elle permet d'en illustrer le principe et l'une des propriétés fondamentales : quelles que soient les dynamiques présentes dans le signal, elles sont analysées avec la même précision absolue.

En pratique, on a souvent des signaux composés de bouffées d'activité de courte durée, contenant des hautes fréquences, superposées à des composantes basses fréquences de longue durée. Il s'avère alors nécessaire de disposer d'une grande résolution temporelle dans les hautes fréquences afin de déterminer les instants d'occurrence de ces bouffées, tandis que dans les basses fréquences, une bonne résolution fréquentielle aura l'avantage de mieux caractériser les composantes de longues durées.

Ce problème peut être résolu en utilisant des fenêtres telles que $\frac{\Delta\nu}{\nu} = Q = cste$. C'est ce que réalise la transformée en ondelettes.

4.1.2 La transformée en ondelettes continue

4.1.2.1 Définition

La transformée en ondelettes continue réalise une projection sur un ensemble de fonctions appelées classiquement ondelettes et dont la construction diffère de celle de la STFT : on remplace la variable de fréquence ν par celle d'échelle a. Cette modification est induite par l'utilisation d'un nouvel opérateur élémentaire pour la construction des vecteurs de base. Partant d'une fonction ψ de $L^2(\mathbb{R})$ de moyenne nulle, l'ondelette mère, ceux-ci sont obtenus par action conjointe des opérateurs de dilatation en échelle :

$$\psi(t) \longmapsto \psi_a(t) = \frac{1}{\sqrt{a}}\psi(\frac{t}{a}) \tag{4.9}$$

et de translation en temps :

$$\psi(t) \longmapsto \psi_\tau(t) = \psi(t-\tau) \tag{4.10}$$

L'opérateur de dilatation fait subir à une fonction ψ, un changement d'échelle de facteur a : cela revient à pratiquer sur le graphe $(t, \psi(t))$ une homothétie de paramètre a sur l'axe des temps et $\frac{1}{\sqrt{a}}$ sur celui des amplitudes. Le choix du facteur multiplicatif $\frac{1}{\sqrt{a}}$ est guidé par la volonté de préserver l'énergie du motif analysant, $< \psi_a, \psi_a >=< \psi, \psi >$. Les atomes s'écrivent donc :

$$\psi_{a,\tau}(t) = \frac{1}{\sqrt{a}}\psi(\frac{t-\tau}{a}) \tag{4.11}$$

et définissent l'espace bidimensionnel : le plan temps-échelle, dans lequel l'information du signal $x(t)$ va être représentée. La transformée en ondelette continue CWT (Continous Wavelet Transform) peut alors être définie par :

$$\begin{array}{l} L^2(\mathbb{R}) \longmapsto L^2(\mathbb{R}^2) \\ x(t) \longmapsto CWT_x(a,t) = \int x(u)\psi^*_{a,t}(u)du =< x(u), \psi_{a,t}(u) > \end{array} \tag{4.12}$$

Cette transformation est inversible, à condition que l'ondelette-mère vérifie la condition, dite d'admissibilité :

$$\int |\Psi(\nu)|^2 \frac{d\nu}{\nu} = C_\Psi < +\infty \tag{4.13}$$

où $\Psi(\nu)$ est la transformée de Fourier de $\psi(t)$. Cette condition signifie que l'ondelette oscille, c'est à dire :

$$\Psi(0) = \int \psi(t)dt = 0 \tag{4.14}$$

La formule d'inversion de cette transformée est alors :

$$x(t) = \frac{1}{C_\psi}\int\int CWT_x(a,\tau)\psi_{a,t}(\tau)\frac{dad\tau}{a^2} \tag{4.15}$$

4.1.2.2 Résolution dans le plan temps-échelle

La condition d'admissibilité donne à la fonction ondelette un caractère de type passe bande qui permet de lui associer une fréquence caractéristique $\nu_\psi = \int_0^\infty \nu|\Psi(\nu)|^2 d\nu$ où $\Psi(\nu)$ est la transformée de Fourier de l'ondelette mère $\psi(t)$.
La transformée de Fourier de l'ondelette ψ_a, dilatée de ψ à l'échelle a, s'écrit $\Psi_a(\nu) = \sqrt{(a)}\Psi(a\nu)$. L'opérateur de dilatation translate donc la fréquence centrale selon :

$$\nu_{\psi_a} = \frac{\nu_\psi}{a} \tag{4.16}$$

On peut donc regarder en fréquence l'axe des échelles en utilisant la transformation :

$$a \longmapsto \nu_{\psi_a} = \frac{\nu_\psi}{a} \tag{4.17}$$

Nous verrons alors l'analyse temps-échelle comme une exploration particulière du plan temps-fréquence.
Les résolutions temporelles et fréquentielles de l'ondelette ψ_a vérifient alors :

$$\begin{cases} \Delta t_{\psi_a} = a\Delta t_\psi \\ \Delta \nu_{\psi_a} = \frac{\Delta \nu_\psi}{a} \end{cases} \tag{4.18}$$

L'aire des cellules élémentaires, appelées logons, qui couvrent le plan temps-échelle est ainsi préservée mais ceux-ci se déforment et s'allongent le long de l'axe temporel à mesure que l'échelle a augmente, comme le montre le pavage présenté figure 4.2. Ce mécanisme de

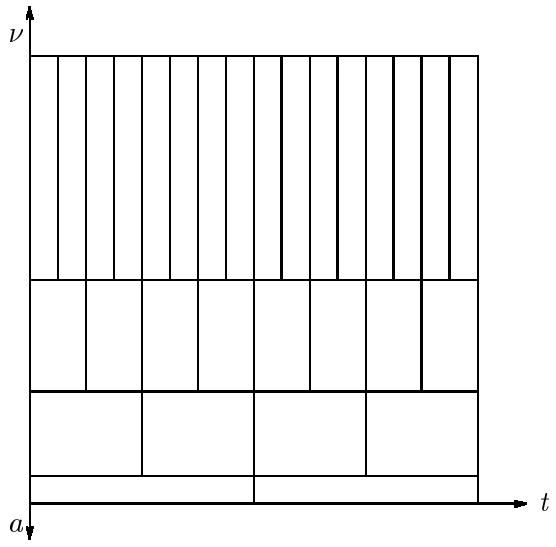


FIG. 4.2 – Pavage du plan temps-échelle

déformation des cellules contient l'essentiel de la richesse de l'analyse temps-échelle. Elle permet, lorsqu'on sélectionne une échelle a petite, d'effectuer une analyse du signal très

localisée en temps (vue de détail) et pour une échelle a grande, de réaliser une analyse sur un horizon beaucoup plus grand (vue d'ensemble). La confrontation des relations précédentes indique que le facteur qualité Q du filtre-ondelette est laissé invariant par action de l'opérateur de dilatation en échelle :

$$Q_{\psi_a} = \frac{\nu_{\psi_a}}{\Delta\nu_{\psi_a}} == \frac{\nu_\psi}{\Delta\nu_\psi} = Q_\psi \tag{4.19}$$

La CWT travaille donc à résolution relative constante. L'analyse des hautes fréquences est réalisée à résolution fréquentielle pauvre, mais permet une localisation temporelle fine (et inversement).

4.1.3 Discrétisation de la CWT

4.1.3.1 Approche intuitive :

On s'aperçoit que si l'on prend une grille d'échantillonnage calquée sur le plan temps-échelle (la grille coïncidant avec le centre des pavés) on obtient une représentation non redondante de l'information. Cette grille est appelée grille dyadique. On démontre qu'un échantillonnage de la transformée continue sur cette grille est critique : il n'y a ni redondance ni perte d'information.

4.1.3.2 La transformée en ondelettes discrète :

La transformée en ondelettes discrète DWT (Discret Wavelet Transform) est donc obtenue par échantillonnage des coefficients d'échelle et de temps sur la grille dyadique :

$$DWT_x(j,k) = CWT_x(a = 2^j, t = 2^j k) = \int x(u)\psi^*_{j,k}(u)du =< x(u), \psi_{j,k}(u) >= d_x(j,k) \tag{4.20}$$

Les ondelettes sont localisées aux noeuds de la grille dyadique :

$$\{\psi_{j,k} = 2^{-j/2}\psi_0(2^{-j}t - k); (j,k) \in \mathbb{Z}^2\} \tag{4.21}$$

et se déduisent de la fonction mère ψ_0 par dilatation en échelle de 2 et par translation. Cette transformée peut être inversée par :

$$x(t) = \sum_j \sum_k d_x(j,k)\check{\psi}_{j,k}(t) \tag{4.22}$$

où $\check{\psi}_{j,k}(t)$ est la base duale de $\psi_{j,k}(t)$. Si on a une base d'ondelettes orthonormale : $\forall(j,k) \in \mathbb{Z}^2, \quad \check{\psi}_{j,k} = \psi_{j,k}$, alors :

$$x(t) = \sum_j \sum_k d_x(j,k)\psi_{j,k}(t) \tag{4.23}$$

Certaines ondelettes peuvent être générées par analyse multi-résolution ou AMR, nous allons voir dans le paragraphe suivant comment les coefficients de la transformée en ondelettes discrète d'un signal peuvent être obtenus par AMR, en nous limitant au cas des ondelettes orthogonales.

4.2 L'Analyse Multi-Résolution

L'analyse multirésolution consiste à projeter le signal x sur une série de sous espaces orthogonaux de $L^2(\mathbb{R})$ (les espaces d'approximations V_i et de détails W_i). Nous verrons que la projection d'un signal sur les espaces de détails fournit sa transformée en ondelettes discrète. Les espaces de projections du signal sont entièrement caractérisés par la donnée de deux filtres (passe haut et passe bas). Ces filtres permettent le calcul rapide des coefficients de la transformée en ondelettes discrète via un algorithme itératif.

4.2.1 Théorie de la MRA

4.2.1.1 Définition

Définition 3 *Une analyse multi-résolution de $L^2(\mathbb{R})$ est une suite $\{V_m\}$ de sous espaces fermés de $L^2(\mathbb{R})$ ayant les propriétés suivantes :*

- *(1) $\bigcap_m V_m = \{0\}$, $\bigcup_m V_m$ est dense dans $L^2(\mathbb{R})$ et $V_{m+1} \subset V_m$*
- *(2) Pour toute fonction $x(t)$ de $L^2(\mathbb{R})$ et tout m de $\mathbb{Z}$, $x(t) \in V_m \Leftrightarrow x(2^m t) \in V_0$*
- *(3) Pour toute fonction $x(t)$ de V_0 et tout k de $\mathbb{Z}$, $x(t-k) \in V_0$*
- *(4) Il existe une fonction $\phi(t)$ de V_0 telle que l'ensemble $\{\phi(t-k)\}_{k\in\mathbb{Z}}$, constitue une base inconditionnelle ou base de Riesz de V_0. C'est à dire qu'il existe deux réels A et B avec $A > 0$, tels que : pour toute fonction f de V_0, $f = \sum_k g_k \phi(t-k)$, et $A\|f\|^2 \leq \sum g_k^2 \leq B\|f\|^2$.*

Interprétations

- (1) Les V_m sont appelés espaces d'approximations. La première relation ($V_{m+1} \subset V_m$) traduit le fait que la projection dans V_{m+1} est une approximation plus grossière du signal que sa projection dans V_m, c'est à dire que l'information contenue dans V_m est plus riche que celle contenue dans V_{m+1}.
- (2) montre que l'on peut passer d'un espace d'approximation à un autre par changement d'échelle.
- (3) est l'invariance par translation temporelle.
- (4) montre que l'on peut engendrer V_0 par translation d'un même motif et assure la stabilité numérique de la décomposition d'une fonction sur V_0.

4.2.1.2 Fonction échelle

La fonction ϕ est appelée fonction d'échelle car elle permet de passer d'un espace d'approximation à un autre, c'est à dire d'une échelle à une autre.

La fonction ϕ et ses versions translatées engendrent l'espace V_0. Un simple changement d'échelle (cf définition (2)), montre que les sous-espaces V_j sont engendrés par la dilatée $\phi_j(t) = \phi(2^{-j}t)$ et ses translatées. Cette famille constitue une base de Riesz de V_j. En général, on normalise ces fonctions : si $\|\phi\|_2 = 1$ alors il en est de même pour $\{\phi_{j,k}(t) = 2^{-j/2}\phi(2^{-j}t - k)\}$, les fonctions génératrices de l'espace d'approximation V_j. Pour un signal x d'énergie finie, les coefficients d'approximations sont définis par :

$$a_x(j,k) =< x, \phi_{j,k} > \tag{4.24}$$

L'approximation du signal x à la résolution 2^{-j} correspond à sa projection dans V_j :

$$A_j x(t) = \sum_k a_x(j,k)\check{\phi}_{j,k}(t) \tag{4.25}$$

4.2.1.3 Espaces de détails

On définit $\{W_i\}$, les ensembles tels que :

$$W_i \oplus V_i = V_{i-1} \tag{4.26}$$

Les W_i représentent les espaces de «détails» (ce sont les complémentaires orthogonaux des espaces d'approximations). Cette construction implique directement que les W_i sont orthogonaux entre eux et que leur somme directe recouvre $L^2(\mathbb{R})$:

$$L^2(\mathbb{R}) = \oplus_{j\in\mathbb{Z}} W_j \tag{4.27}$$

En fréquence, on observe mieux la complémentarité des deux ensembles ainsi que leur finalité (basses fréquences correspondant à approximation, hautes fréquences à détail) : Soit $f \in V_1$, soit g tel que $g(t) = f(2t) \in V_0$, alors en transformée de Fourier on a :

$$G(\omega) = \int f(2t)e^{-i\omega t}dt \tag{4.28}$$

$$G(\omega) = \frac{1}{2}F(\frac{\omega}{2}) \tag{4.29}$$

La figure 4.3 montre la géométrie de ces espaces dans le long de l'axe des fréquences.

4.2.1.4 Fonction ondelette

Un des principaux résultats de l'AMR fournit l'existence de la fonction ψ telle que $\{\psi(t-k)\}$ est une base de W_0. Cette fonction est appelée ondelette mère. La famille

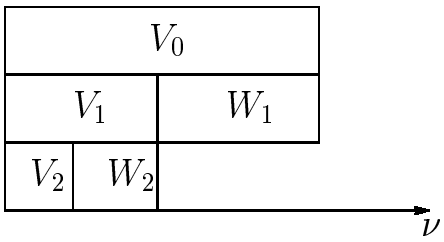


FIG. 4.3 – Schéma de la géométrie des espaces de détails et d'approximations

$\{\psi_{j,k}(t) = 2^{-j/2}\psi(2^{-j}t - k)\}$ constitue alors une base de Riesz de W_j.
Pour un signal x d'énergie finie, les coefficients de détails sont définis par :

$$d_x(j,k) =< x, \psi_{j,k} > \tag{4.30}$$

Le détail du signal x à la résolution 2^{-j} correspond à sa projection dans W_j :

$$D_j x(t) = \sum_k d_x(j,k)\check{\psi}_{j,k}(t) \tag{4.31}$$

La relation 4.26 signifie que l'approximation du signal à un niveau j correspond à une approximation plus grossière complétée par le détail :

$$A_j x(t) = A_{j+1}x(t) + D_{j+1}x(t) \tag{4.32}$$

Et la relation 4.27 implique que pour tout signal x de $L^2(\mathbb{R})$

$$x(t) = \sum_j D_j x(t) = \sum_j \sum_k d_x(j,k)\check{\psi}_{j,k}(t) \tag{4.33}$$

Du fait de la structure emboîtée des espaces (V_i et W_i sont inclus dans V_{i-1}), il existe une relation d'échelle entre ces espaces. Les fonctions ϕ et ψ définissant ces espaces, elles respectent cette relation que nous présentons au paragraphe suivant.

4.2.1.5 Relation à deux échelles

Cette relation est appelée ainsi car elle fait intervenir deux échelles distinctes dans son écriture, c'est à dire qu'elle fait le lien entre deux espaces consécutifs.
$V_1 \subset V_0$, alors $\phi_{1,0} = \phi(\frac{t}{2}) \in V_1$ est combinaison linéaire des $\phi(t-k)$ (base de V_0), d'où :

$$\forall l \in \mathbb{Z}, \exists g(l), \forall t \in \mathbb{R}, \phi(\frac{t}{2}) = \phi_{1,0} = \sum g(l)\phi(t-l) = g * \phi(t) \tag{4.34}$$

La fonction ψ respecte aussi la relation à deux échelles : En effet, $\psi(\frac{t}{2}) \in W_1 \subset V_0$ est combinaison linéaire des $\phi(t-k)$.

$$\forall l \in \mathbb{Z}, \exists h(l), \forall t \in \mathbb{R}, \psi(\frac{t}{2}) = \psi_{1,0} = \sum h(l)\phi(t-l) = h * \phi(t) \tag{4.35}$$

Ces relations mettent en évidence l'existence d'un filtre passe haut h et d'un passe bas g dont la donnée est équivalente à celle des fonctions ondelette et échelle. Ces filtres nous permettront de réaliser la transformée en ondelettes discrète directement par filtrage du signal en appliquant l'algorithme présenté au paragraphe 4.2.3.

4.2.2 La transformée en ondelettes discrète

4.2.2.1 Définition

La transformée en ondelettes discrète d'un signal $x(t)$ est définie par la collection de ses coefficients de détails $\{d_x(j,k)\}_{(j,k)\in\mathbb{Z}}$, projections orthogonales de x dans les espaces définis par l'AMR.

$$\begin{array}{ccc} L^2(\mathbb{R}) & \longmapsto & l^2(\mathbb{Z}) \\ x(t) & \longmapsto & d_x(j,k) =< x, \psi_{j,k} > \end{array} \tag{4.36}$$

Cette transformée peut être inversée à l'aide d'une somme discrète, qui met en jeu la base duale $\{\check{\psi}\}(j,k) \in \mathbb{Z}$:

$$x(t) = \sum_j \sum_k d_x(j,k)\check{\psi}_{j,k}(t) \tag{4.37}$$

Les quatre relations données par la définition 3, confèrent à la fonction ψ son statut d'ondelette.

4.2.2.2 Remarques

Il y a plusieurs avantages à utiliser l'AMR pour générer l'ondelette ψ :
- elle permet d'expliciter la base duale
- elle rend utilisable la formule de reconstruction exacte
- la base duale est une base d'ondelettes
- dans le cas d'ondelettes orthogonales, la base duale est la base de départ ($\check{\psi} = \psi$).

De plus, la transformée d'un signal en ondelettes discrète peut être obtenue par filtrages et décimations successifs. C'est ce que nous allons présenter au paragraphe suivant.

4.2.3 Algorithme pyramidal

4.2.3.1 Présentation de l'algorithme

Nous avons vu que l'AMR d'un signal revient à le décomposer à différentes échelles, en approximations et en détails. S. Mallat [45] propose un algorithme rapide permettant de calculer les coefficients de détails et d'approximations en utilisant des filtrages et décimations successifs.

La figure 4.4 présente cet algorithme : Les coefficients de détails correspondant à l'espace W_1 sont obtenus par filtrage passe haut (filtre $h1$) puis décimation par 2, les approximations sont obtenues de la même manière par filtrage passe bas (g_1). Pour

obtenir les coefficients de détails aux résolutions supérieures, il suffit de réitérer ces étapes sur les coefficients d'approximations.

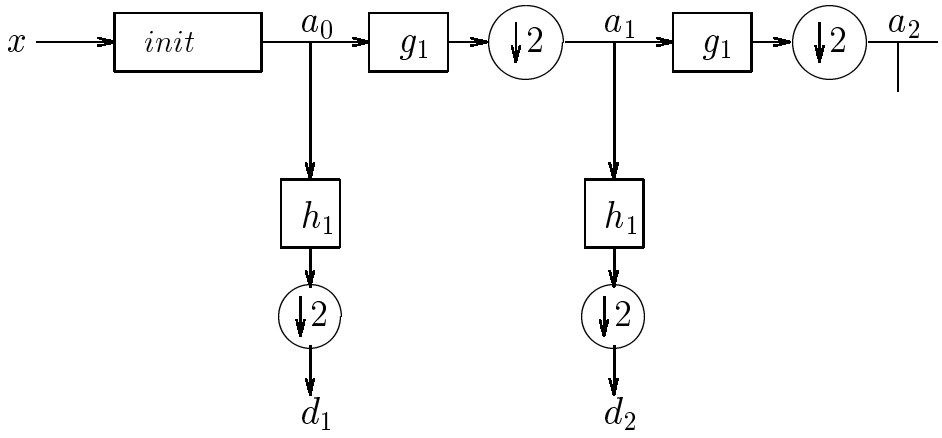


FIG. 4.4 – Algorithme pyramidal de Mallat où les a_i sont les coefficients d'approximations, les d_i ceux de détails.

On peut reconstruire le signal grâce à des filtres h_2 et g_2 selon l'algorithme présenté à la figure 4.5. L'approximation a_n à un niveau donné n est la somme des coefficients de détails d_{n+1} et d'approximations a_{n+1} du niveau supérieur préalablement filtrés et réechantillonés.

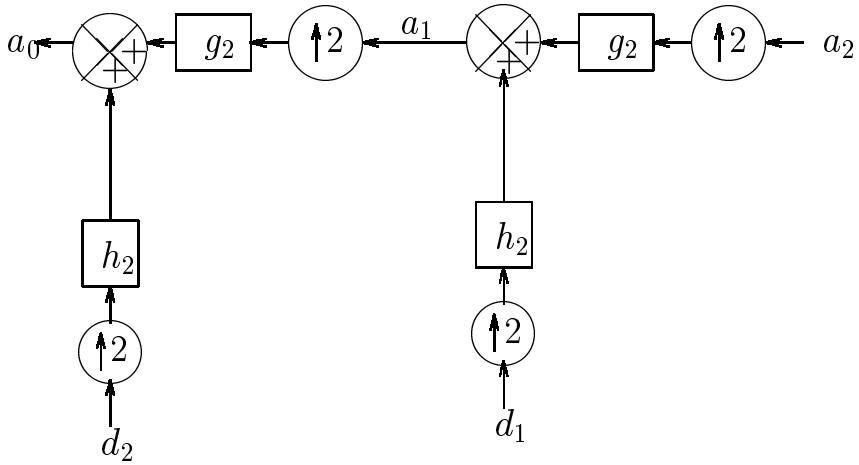


FIG. 4.5 – Algorithme de reconstruction du signal.

Initialisation L'étape d'initialisation consiste à projeter le signal x sur l'espace V_0. Dans la pratique, on dispose du signal échantillonné, on choisit alors la solution d'approximer $a_{0,k}$ par $x[k]$. Dans notre cas, nous utiliserons les ondelettes de Coifman afin de diminuer cette erreur d'approximation [45].

4.2.3.2 Filtrage par bande

D'un point de vue fréquentiel, le signal apparaît comme décomposé suivant différentes bandes. La figure 4.6 présente ce point de vue.

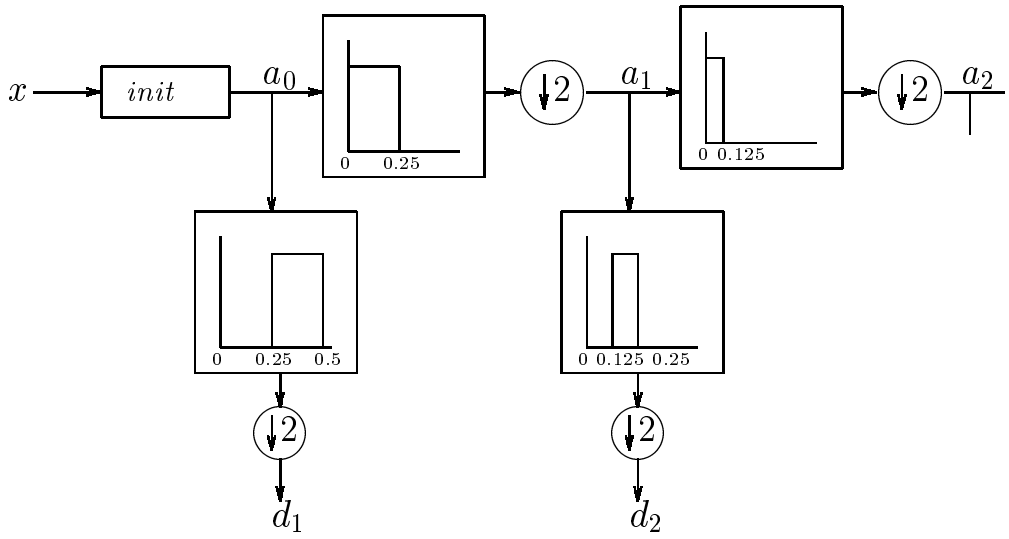


FIG. 4.6 – Algorithme pyramidal de Mallat : point de vue fréquentiel

Les filtres h_1 et g_1 sont liés aux filtres exhibés par les relations à deux échelles 4.34 et 4.35. Les conditions imposées par la définition de l'AMR impliquent que le filtre g soit passe bas, on a de plus :

$$\begin{cases} h_1(k) = \bar{h}(k) = h(-k) \\ g_1(k) = \bar{g}(k) = g(-k) \end{cases} \tag{4.38}$$

Les filtres de reconstruction h_2 et g_2 sont liés aux fonctions des bases duales. Dans le cas où les bases sont orthonormales on a :

$$\begin{cases} h_2(k) = h(k) \\ g_2(k) = g(k) \end{cases} \tag{4.39}$$

dans le domaine fréquentiel :

$$|H(\omega)|^2 + |H(\omega+\pi)|^2 = 2 \tag{4.40}$$

$$|H(\omega)| = |G(\omega+\pi)| = |G(\omega-\pi)| \tag{4.41}$$

$$|H(\omega)|^2 + |G(\omega)|^2 = 2 \tag{4.42}$$

Les filtres sont alors symétriques par rapport à $\pi/2$, de puissances complémentaires. Ce sont des filtres miroirs en quadrature (QMF, Quadrature Mirror Filter).

4.2.4 Conclusion

Nous avons présenté la théorie de l'analyse multirésolution en utilisant les fonctions ondelettes et échelles. Dans notre cas, nous pouvons insister l'importance de la relation

à deux échelles et donc celle des coefficients des filtres g et h, c'est à dire celle des filtres. Ce sont en effet les choix sur les filtres qui vont déterminer les ondelettes associées. Ce sont aussi ces filtres qui permettent de représenter au mieux la décomposition en sous bandes du signal.

La figure 4.7 présente la décomposition en base d'ondelettes du signal x composé de N points. L'arbre de décomposition a $\log_2(N)$ niveaux. A chaque niveau, la résolution temporelle est divisée par 2, au dernier niveau les coefficients de détails sont représentés par un unique point, la résolution temporelle est nulle et la résolution fréquentielle est maximum. Le signal est décomposé en $N-1$ coefficients de détails et 1 coefficient d'approximation (la composante la plus basse fréquence du signal). La figure 4.8 représente le pavage du plan temps fréquence induit par la décomposition d'un signal $x \in \mathbb{R}^{16}$.

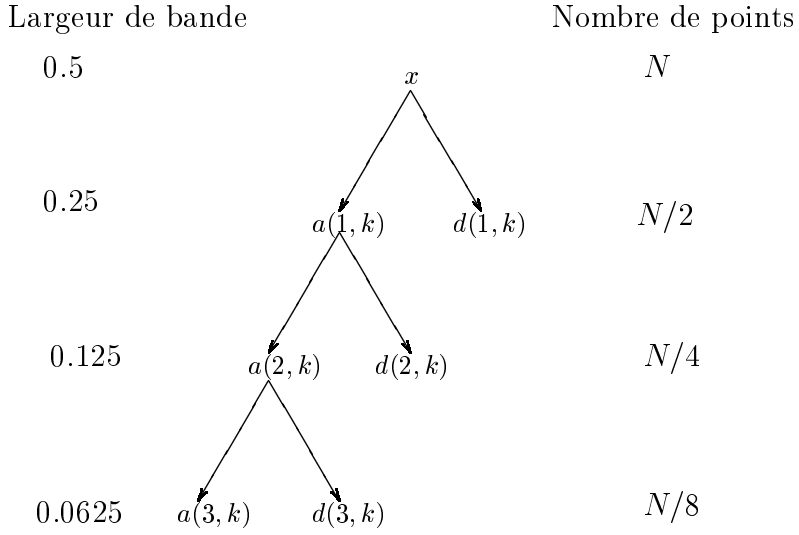


FIG. 4.7 – Arbre de décomposition d'un signal sur une base d'ondelettes

4.3 Généralisation aux images

La généralisation de l'AMR aux signaux de plusieurs dimensions ne pose aucune difficulté d'ordre théorique si l'on utilise des ondelettes séparables : Soient ϕ et ψ les fonctions échelle et ondelette générant une bases d'ondelettes orthonormales de $L^2(\mathbb{R})$, on définit les fonctions ondelettes séparables à deux dimensions de la façon suivante :

$$\psi^1(x,y) = \phi(x)\psi(y), \quad \psi^2(x,y) = \psi(x)\phi(y), \quad \psi^3(x,y) = \psi(x)\psi(y) \tag{4.43}$$

En reprenant les notations utilisées précédemment :

$$\text{pour } 1 \leq i \leq 3, \quad \psi^i_{j,n,m}(x,y) = \frac{1}{2^j}\psi^i(\frac{x-2^j n}{2^j}, \frac{y-2^j m}{2^j}) \tag{4.44}$$

alors la famille d'ondelettes

$$\{\psi^1_{j,n,m}(x,y), \psi^2_{j,n,m}(x,y), \psi^3_{j,n,m}(x,y)\}_{j,n,m\in\mathbb{Z}^3} \tag{4.45}$$

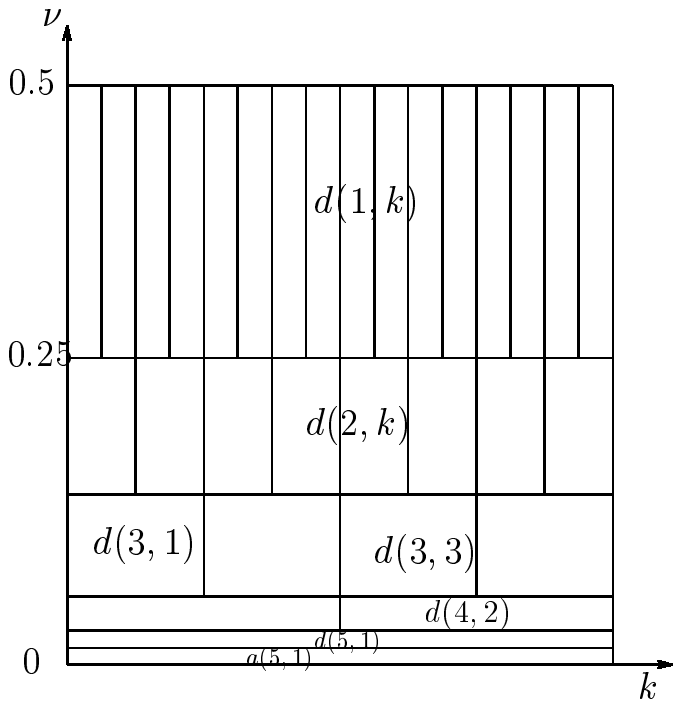


FIG. 4.8 – Pavage du plan temps fréquence correspondant à la décomposition d'un signal $x \in \mathbb{R}^{16}$ sur une base d'ondelettes.

définit une base biorthonormale de $L^2(\mathbb{R}^2)$.
La fonction échelle associée est $\phi^0(x,y) = \phi(x)\phi(y)$.

En pratique, pour calculer les coefficients d'approximations et de détails d'une image I, nous utilisons la généralisation de l'algorithme pyramidal présenté paragraphe 4.2.3. Chaque étape de cet algorithme est appliquée successivement aux lignes puis aux colonnes de l'image. La figure 4.9 présente la version «2D» de l'algorithme. On obtient pour un niveau de décomposition une imagette d'approximations $a_j(n,m)$ et trois imagettes de détails $d_j^1(n,m), d_j^2(n,m), d_j^3(n,m)$ selon l'orientation fréquentielle (horizontale, verticale et diagonale).

L'arbre de décomposition quaternaire est représenté sur la figure 4.10. La décomposition est représentée sous la forme d'une image où les basses fréquences sont en haut à gauche, les hautes en bas à droite (cf figure 4.11). Les figures 4.12 et 4.13 présentent cette décomposition pour l'image Lenna et une image composée d'une croix diagonale dans un carré. Cette dernière figure permet d'observer les orientations fréquentielles des coefficients de détails.

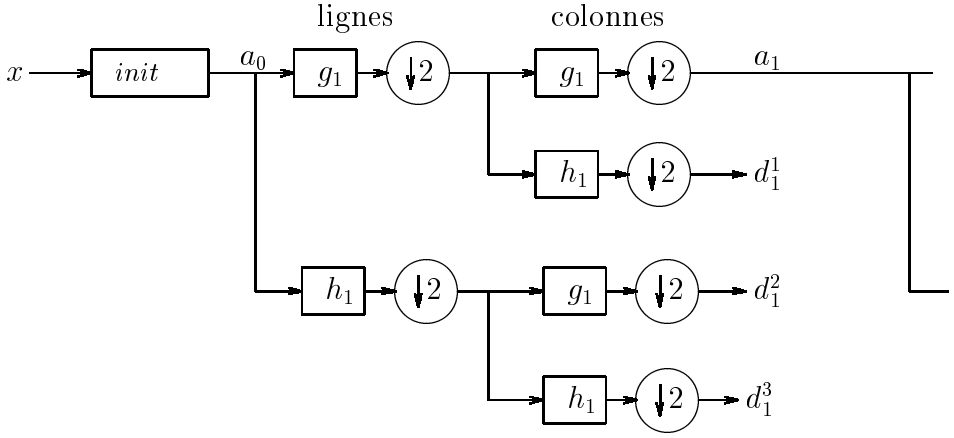


FIG. 4.9 – Algorithme pyramidal de décomposition d'une image en coefficients d'approximations et de détails, on applique les filtrages et décimations successivement selon les lignes puis les colonnes.

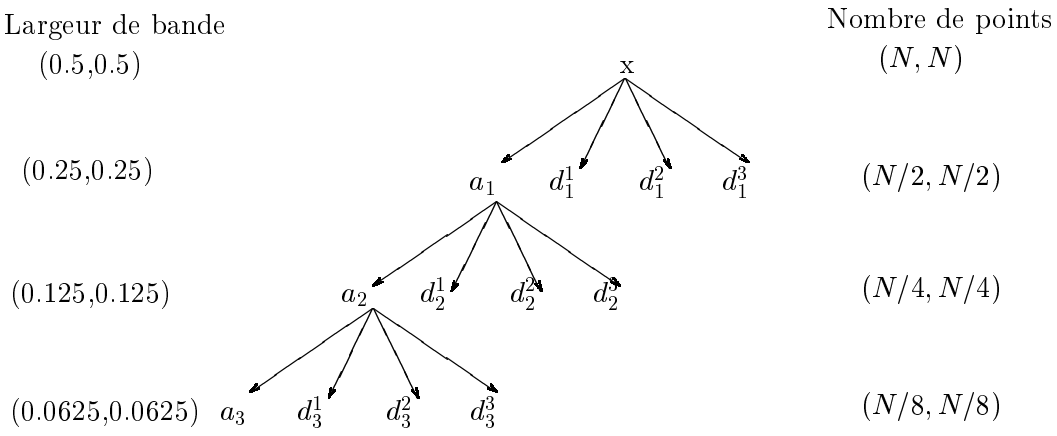


FIG. 4.10 – Arbre de décomposition d'une image sur une base d'ondelettes

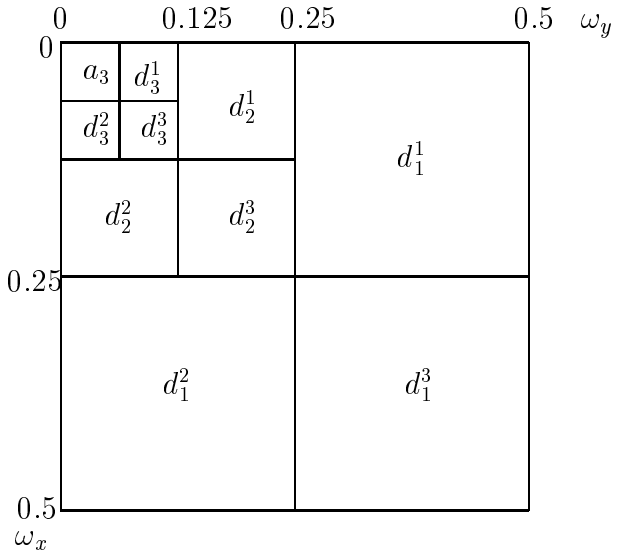


FIG. 4.11 – Disposition des coefficients de décomposition d'une image pour la profondeur 3

FIG. 4.12 – Exemple de transformée en ondelettes pour l'image Lenna, les niveaux de gris ont été normalisés.

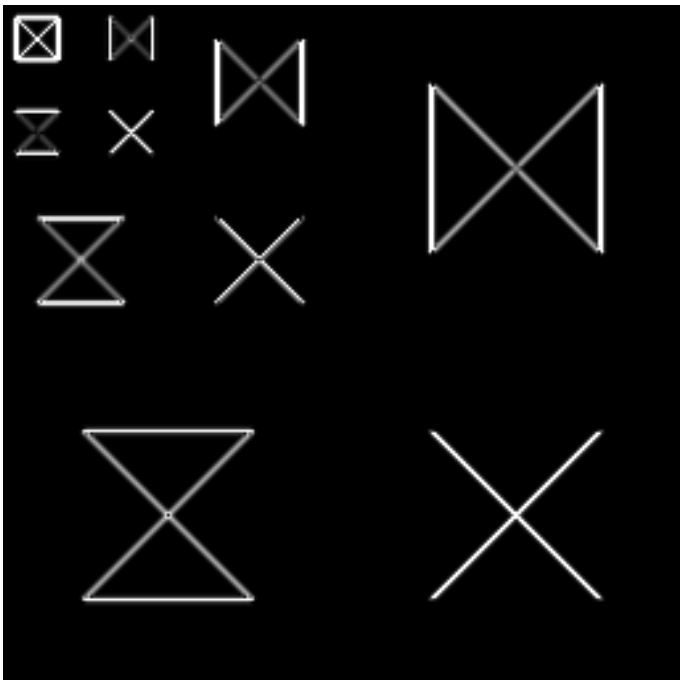


FIG. 4.13 – Exemple de transformée en ondelettes pour l'image «BoxWithCross», les niveaux de gris ont été normalisés.

Chapitre 5

Décomposition en paquets d'ondelettes, sélection de meilleure base

Le chapitre précédent a introduit la transformée en ondelettes discrète d'un signal et d'une image. Si l'on adopte un point de vue fréquentiel, la transformée en ondelettes peut être assimilée à une segmentation fréquentielle de l'information contenue dans le signal à la manière d'un banc de filtres présentant une structure dyadique. La répartition de la résolution dans le plan temps-échelle est ainsi figée (voir les figures 4.8 et 4.11) et peut ne pas répondre à tous les besoins.

Le principe de la décomposition d'un signal sur une base de paquets d'ondelettes consiste à s'affranchir de la structure dyadique du pavage temps-fréquence induite par la transformée en ondelettes discrète. Pour ce faire, on généralise la théorie de l'AMR en créant des nouveaux espaces de projections orthogonaux issus de la décomposition des sous-espaces de détails W_i. Ces sous espaces sont organisés selon une architecture d'arbre binaire. La projection du signal sur l'ensemble des sous espaces constitue la décomposition du signal en paquets d'ondelettes. Celle-ci étant fortement redondante, il est loisible de sélectionner une base de paquets d'ondelettes représentant le signal. Généralement, la sélection de la base de représentation est faite selon les caractéristiques du signal traité et des critères se rapportant à l'application désirée. Cette base est alors appelée «meilleure base».

Dans ce chapitre, nous présenterons les principes de la décomposition d'un signal en paquets d'ondelettes et nous définirons les bases de paquets d'ondelettes. La deuxième partie de ce chapitre sera consacrée à la présentation d'exemples d'algorithmes de sélection de meilleure base. En particulier, nous développerons l'algorithme nous permettant de choisir une meilleure base pour le tatouage d'images.

5.1 Décomposition en paquets d'ondelettes, bases de paquets d'ondelettes

5.1.1 Décomposition en paquets d'ondelettes

La décomposition en paquets d'ondelettes du signal est une généralisation de l'Analyse multi-résolution. Les espaces d'approximations sont toujours découpés de la même façon mais les espaces de détails sont eux aussi somme directe de deux sous espaces de résolutions temporelles inférieures (divisées par 2). On démontre l'orthogonalité de ces sous espaces. Nous ne développerons pas ici l'aspect théorique de cette décomposition mais nous nous intéresserons au côté applicatif.

Généralisation de l'AMR

Le principe de la décomposition en paquets d'ondelettes est de réitérer le processus de décomposition d'un signal en approximation et en détails non plus uniquement sur les coefficients d'approximations mais aussi sur ceux de détails. On dispose alors d'un plus grand nombre d'espaces de projection.

La figure 5.1 représente l'algorithme pyramidal étendu permettant d'obtenir les coefficients. Comme pour le calcul rapide des coefficients de la transformée en ondelettes d'un signal, on procède par filtrages et décimations successives du signal. Ici, les coefficients de détails sont aussi décomposés.

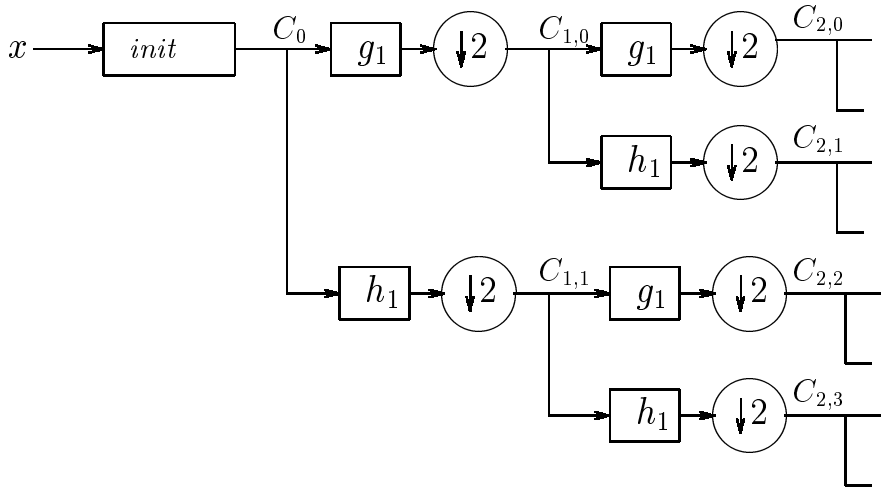


FIG. 5.1 – Schéma de l'algorithme de la décomposition en paquets d'ondelettes d'un signal, les coefficients sont obtenus par filtrages successifs passe haut (filtre h_1) et passe bas (filtre g_1) puis décimation du signal.

Notations

g_1 et h_1 sont les filtres QMF associés aux fonctions échelle ϕ et ondelette ψ. On appelle paquets d'ondelettes les $C_{i,j}$. Chaque paquet $C_{i,j}$ contient $n/2^{-j}$ coefficients dans le cadre de la décomposition d'un signal de longueur n. Les coefficients des paquets d'ondelettes sont notés $C_{j,m}(k)$, où j est le niveau de résolution, m correspond à la bande spectrale, k est l'indice de translation. Ils sont obtenus par la décomposition du signal sur les bases engendrées par les fonctions W_m :

$$C_{j,m}(k) =< x(t), 2^{-j/2} W_m(2^{-j}t - k) > \tag{5.1}$$

$$W_{2m}(t) = 2^{1/2} \sum_k g_k W_m(2t - k) \tag{5.2}$$

$$W_{2m+1}(t) = 2^{1/2} \sum_k h_k W_m(2t - k) \tag{5.3}$$

où

- W_0 correspond à la fonction ϕ
- W_1 correspond à la fonction ψ

Redondance de l'information

La figure 5.2 présente l'arbre binaire de décomposition en paquets d'ondelettes pour un signal d'une dimension.

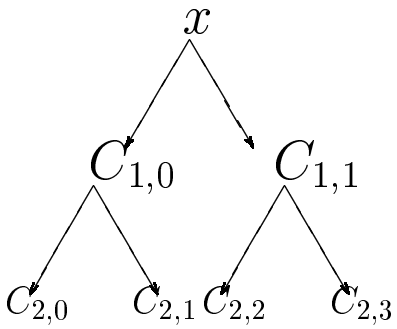


FIG. 5.2 – Arbre binaire de décomposition d'un signal en paquets d'ondelettes

A chaque niveau de l'arbre, toute l'information du signal est représentée. A un niveau de décomposition donné, correspond un découpage fréquentiel régulier. Au dernier niveau, chaque fréquence est représentée par un point, on a perdu toute l'information temporelle, on a une décomposition purement fréquentielle du signal. La figure 5.3 montre le pavage du plan temps-fréquence pour un signal $x \in \mathbb{R}^8$ pour chacun des niveaux de l'arbre.

5.1.2 Bases de paquets d'ondelettes

L'arbre binaire de décomposition en paquets d'ondelettes donne donc une représentation fortement redondante du signal. Si l'on souhaite travailler avec une représentation

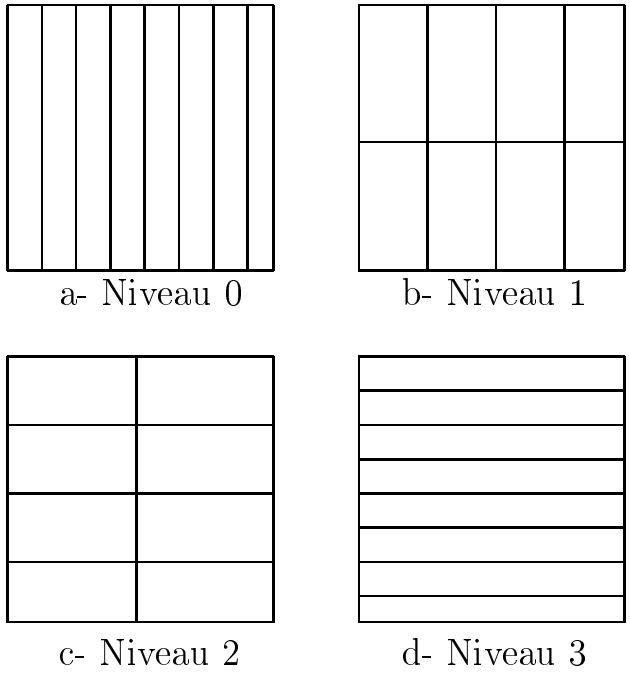


FIG. 5.3 – Pavages temps fréquences correspondant à chaque niveau de l'arbre de décomposition

non redondante, il faut choisir une base de paquets, c'est à dire un ensemble de noeuds de l'arbre dont la projection dans l'espace temps-fréquence forme une partition. Celle-ci est obtenue à partir de la notion d'arbre admissible. Un arbre admissible est composé de noeuds ayant 0 ou 2 fils, la base sera constituée de tous les noeuds n'ayant pas de fils. En considérant le découpage fréquentiel induit par la décomposition en paquets d'ondelettes, cela revient à recouvrir l'axe des fréquences sans chevauchement.

La figure 5.4 représente deux exemples de bases de paquets d'ondelettes. Les noeuds choisis dans la constitution de la base sont entourés par des carrés. On voit que si on élague les arbres au niveau des noeuds choisis, on obtient des arbres admissibles. Les paquets choisis forment bien une partition de l'axe des fréquences (en horizontal sur l'arbre). Le pavage du plan temps-fréquence induit par les bases est représenté pour un signal $x \in \mathbb{R}^8$.

Reconstruction

La décomposition en base de paquet d'ondelettes découlant du principe de l'AMR, on peut reconstruire le signal en utilisant les filtres de reconstruction associés aux filtres de décomposition. Si $\check{W}_m$ est la base duale associée aux fonctions W_m, et B est l'ensemble des indices $\{j, m\}$ des noeuds sélectionnés dans une base de paquets d'ondelettes, alors

$$x(t) = \sum_{\{j,m\} \in B} \sum_{k} C_{j,m}(k) \frac{1}{2^{j/2}} \check{W}_m(2^{-j}t - k) \tag{5.4}$$

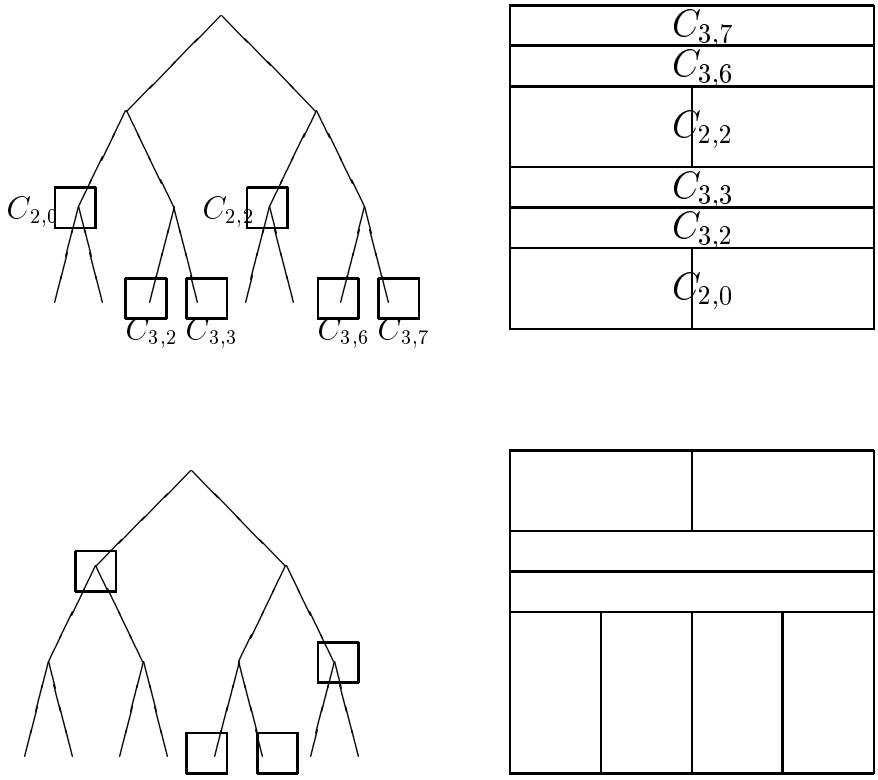


FIG. 5.4 – Exemples de bases de paquets d'ondelettes et pavages temps fréquences correspondants

Meilleures bases

Obtenir la «meilleure» base de décomposition, revient à rechercher l'ensemble des coefficients d'approximations et de détails les mieux adaptés pour représenter le signal et l'information qui nous intéresse. Nous présenterons des exemples d'algorithmes de sélection de meilleure base dans la seconde partie de ce chapitre.

5.1.3 Généralisation aux images

La décomposition d'une image sur une base de paquets d'ondelettes suit le même principe que la décomposition d'un signal monodimensionel. On généralise l'algorithme de décomposition en ondelettes en filtrant et décimant les coefficients de détails et d'approximations. Dans le cas des images, on agit sur les lignes et les colonnes, on aura alors l'arbre quaternaire de décomposition en paquets d'ondelettes représenté figure 5.5.

Dans la représentation quaternaire en paquets d'ondelettes, chaque paquet $C_{p,i,j}$ correspondant à un noeud de l'arbre contient l'information relative à toute l'image dans la bande de fréquence indicée par (i, j) et dont la taille est déterminée par le niveau de résolution p. Les coefficients du paquet sont notés $C_{p,i,j}(k, l)$.

Cette décomposition peut être interprétée comme la décomposition en sous bandes

de l'image, à des résolutions fréquentielles croissantes. La figure 5.6 (a, b et c) présente le découpage spatio-fréquentiel obtenu pour les trois premiers niveaux de l'arbre. Comme expliqué précédemment, la décomposition obtenue est redondante, on peut sélectionner à partir de l'arbre et d'un critère, une meilleure base de paquets d'ondelettes. La figure 5.6 (c) présente une base possible de paquets d'ondelettes.

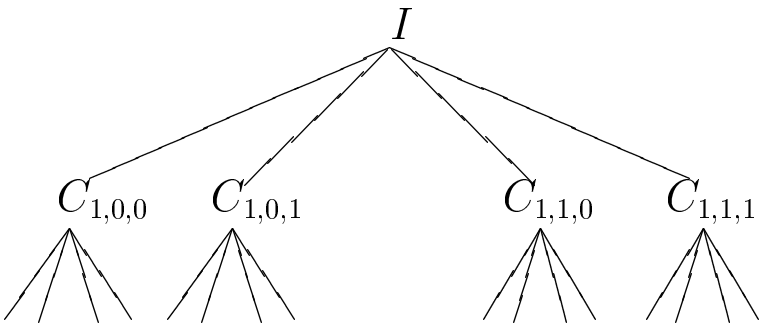


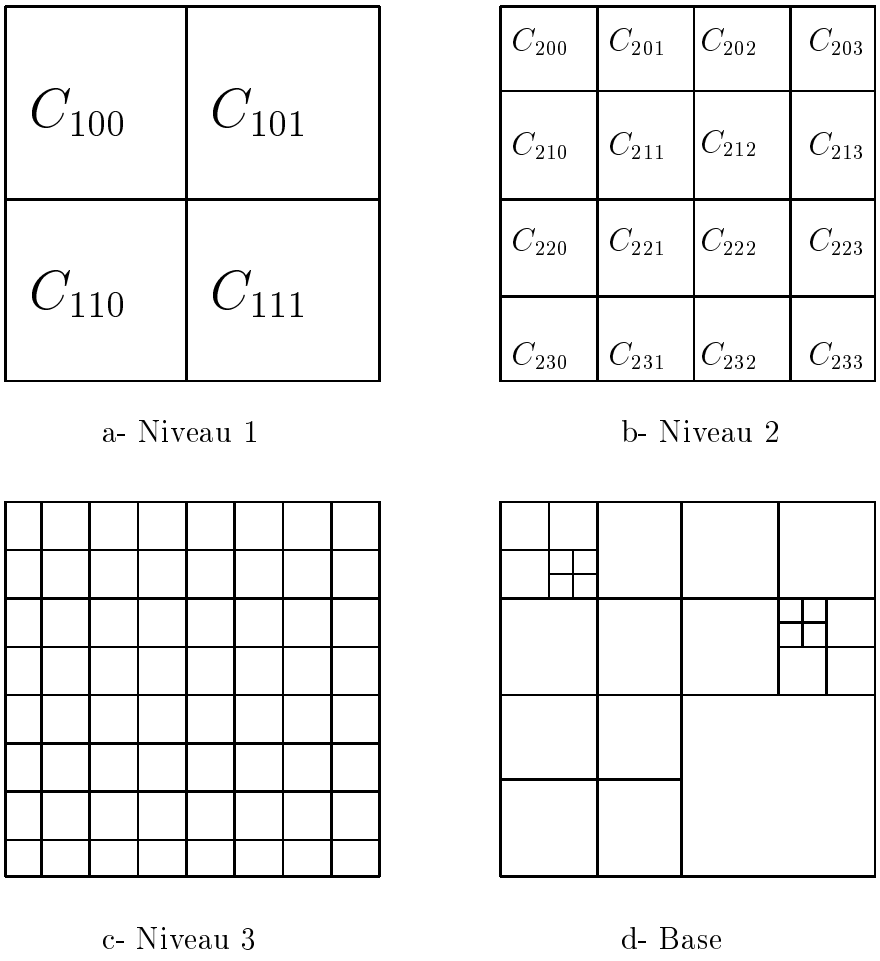
FIG. 5.5 – Arbre quaternaire de décomposition en paquets d'ondelettes. Les coefficients des paquets sont obtenus par filtrages et décimations successifs selon les lignes et les colonnes.

5.1.4 Conclusion

Nous avons vu que la décomposition en paquets d'ondelettes d'un signal conduit à de nombreux choix possibles de bases, parmi lesquelles une «meilleure» base pourra être déterminée. La sélection de cette meilleure base sera faite en fonction du signal et de l'information recherchée. Nous allons maintenant étudier différents algorithmes de sélection de meilleure base concernant diverses applications : compression, classification et détection de ruptures, puis nous présenterons l'algorithme proposé pour le tatouage d'images.

5.2 Sélection de meilleures bases de décomposition en paquets d'ondelettes

La notion de meilleure base de paquets d'ondelettes a été introduite par Coifman et Wickerhauser [51] dans le cadre de la compression des signaux. L'idée principale est de trouver une base qui représente le mieux le signal, c'est à dire sur laquelle l'information sera la plus concentrée. Dans la mesure où la plupart des algorithmes de sélection d'une base suivent les étapes mises en place dans cette méthode, nous allons commencer par la détailler. Nous présenterons ensuite d'autres algorithmes de sélection de base concernant les applications de débruitage, de classification supervisée et de détection de ruptures fréquentielles. Nous conclurons ce chapitre en décrivant l'algorithme que nous avons choisi de développer dans le cadre du tatouage d'images.



a- Niveau 1 b- Niveau 2

c- Niveau 3 d- Base

FIG. 5.6 – a,b,c : Découpages espace-fréquence correspondant aux trois premiers niveaux de la décomposition en paquets d'ondelettes. d : exemple de meilleure base

5.2.1 Sélection d'une meilleure base pour la compression

L'algorithme de sélection de meilleure base de paquets d'ondelettes a été tout d'abord mis en place pour la compression [51] [52]. Il est constitué de deux étapes. La première consiste à déterminer un critère permettant d'exprimer mathématiquement les objectifs de l'application désirée. Dans le cadre de la compression des signaux, on veut maximiser la concentration de l'énergie sur un petit nombre de vecteurs. Le critère sera une fonction de coût additive permettant de mesurer cette concentration de l'information, comme par exemple l'entropie du signal.

La deuxième étape de l'algorithme consiste à adopter une stratégie de recherche de la base permettant d'optimiser ce critère. Une méthode brutale consiste à calculer les projections du signal sur toutes les bases possibles puis à choisir celle qui minimise le critère. Or, pour un arbre de longueur j, le nombre de bases possibles N_B est trop important pour espérer faire ce calcul : $2^{2^{j-1}} \leq N_B \leq 2^{\frac{5}{4}2^{j-1}}$. Coifman *et al.* ont adopté une stratégie de recherche locale du minimum du critère. Le critère étant une fonction additive, on peut en effet travailler sur l'arbre de décomposition en paquet d'ondelettes de façon locale : L'idée est de calculer l'arbre binaire de décomposition en paquets d'ondelettes et de construire un arbre dans lequel chaque feuille contient la valeur du critère pour le paquet correspondant. L'arbre obtenu pour cette application est appelé arbre entropique. La sélection de la base se fera sur cet arbre en comparant la valeur d'un noeud avec celle de ses fils. Ces étapes sont détaillées ci-dessous :

Algorithme de sélection de la meilleure base

- On décompose le signal x en paquets d'ondelettes
- On calcule le critère entropique en chaque noeud (j, m) :
  $\mathcal{M}_x(j,m) = -\sum p_i \log(p_i)$ avec $p_i = \frac{\|C_{j,m}(i)\|^2}{\|x\|^2}$.
  On obtient l'arbre «entropique»
- On sélectionne la meilleure base en ne conservant que les noeuds qui minimisent le critère de la manière suivante : en partant des extrémités de l'arbre et en remontant vers la racine, pour chaque noeud, on compare son entropie à la somme des entropies de ses fils. Si elle est supérieure, on sélectionne les fils et on remplace l'entropie du père par celle de ses deux fils, sinon on conserve le père.

La stratégie de recherche des noeuds constituant la base s'effectue donc à partir du bas de l'arbre en prenant comme base initiale le dernier niveau. On raisonne ensuite par comparaison : selon la valeur des noeuds on sélectionnera dans la base soit un père, soit ses deux fils. Cette stratégie assure que l'on obtienne une base de paquets d'ondelettes. On peut remarquer que lorsque l'arbre est parcouru, la racine contient la valeur de l'entropie de la projection du signal sur la meilleure base.

Débruitage Une méthode très proche de celle explicitée ci-dessus a été utilisée pour le débruitage de signaux. En effet, si le signal est projeté sur la meilleure base pour la compression, le signal utile est représenté par peu de coefficients de grandes amplitudes

alors que le bruit (supposé la plupart du temps additif gaussien) est réparti sur tous les coefficients de paquets d'ondelettes. Un seuillage permettra donc de diminuer les contributions du bruit dans le signal reconstruit. Donoho [53] *et al.* proposent un critère de sélection de meilleure base fondé sur la fonction de «dimension théorique» du signal liée à un seuil optimal calculé pour le débruitage (voir [53]).

5.2.2 Sélection d'une meilleure base pour la classification supervisée

La méthode de Saito et Coifman [54] est inspirée de la méthode développée pour la compression. Le but est de trouver la base qui sépare le mieux différentes classes de signaux. Le critère utilisé sera donc un critère de discrimination. L'entropie relative ou «cross entropy» constitue une mesure de distance entre les distributions d'énergie de deux séquences x et y, elle est définie par $D(x,y) = \sum_i p_i \log(\frac{p_i}{q_i})$ où $p_i = \frac{|x_i|}{\|x\|^2}$ et $q_i = \frac{|y_i|}{\|y\|^2}$. Cette entropie (aussi appelée information de Kullback) constituera le critère à optimiser. Les étapes de l'algorithme sont les suivantes :

- Les classes d'apprentissage sont chacunes représentées par un arbre moyen. Il contient pour chaque noeud, une séquence de paquets moyenne des carrées des coefficients des individus de la classe.
- Si on a deux classes, l'arbre de décision est alors directement calculé en utilisant l'information de Kullback. Sinon, le critère est obtenu en sommant les mesures calculées sur chacun des couples de classes.
- Le critère étant additif, on applique la stratégie explicitée pour la compression, on trouve alors la base qui sera la plus discriminante pour ces classes de signaux.

Afin de réduire encore la dimension du problème, on peut construire les classifieurs en ne retenant de la meilleure base que les vecteurs les plus discriminants. Cette méthode a été appliquée à des signaux d'électromyographie [55].

5.2.3 Sélection d'une meilleure base pour la détection de ruptures fréquentielles

Le but recherché est de détecter des ruptures fréquentielles dans des signaux multicomposantes stationnaires par morceaux. Pour cela, on décompose le signal en paquets d'ondelettes, puis on cherche une «meilleure» base qui permette de séparer les différents modes du signal tout en gardant le maximum d'information temporelle. On reconstruit ensuite séparément les signaux monocomposantes obtenus grâce à cette meilleure base. Enfin on leur applique un détecteur de rupture.

La stratégie utilisée ici est différente de celle proposée pour la compression. En effet, si le critère entropique permet de séparer les différents modes du signal, il réalise une représentation concentrée du signal. La base correspondant à ce critère induira donc une localisation fréquentielle très précise des modes du signal au détriment de la localisation temporelle. Or, c'est cette localisation qui porte l'information qui nous intéresse. Hitti

[44] a présenté un critère permettant de séparer les modes du signal tout en conservant le plus de résolution temporelle.

La sélection de la meilleure base a lieu en trois étapes. La première consiste à localiser les noeuds de la base correspondant à une activité significative du signal : un critère énergétique permet de décider si le noeud est d'énergie significative. La seconde étape permet de calculer le nombre de composantes présentes dans chaque paquet. La dernière étape sélectionne les paquets monocomposantes de plus grande résolution temporelle, c'est à dire les plus élevés dans l'arbre.

La figure 5.7 décrit sur un exemple les trois étapes de sélection de la meilleure base. La première étape consiste à initialiser l'arbre de décision : on met à 1 les paquets dont les coefficients ont une énergie supérieure à un seuil s, à 0 les autres. On suit ainsi l'évolution de la répartition de l'énergie au sein de l'arbre. La deuxième étape consiste à identifier les paquets multicomposantes. Le nombre de modes d'un noeud est supérieur ou égal à celui de la somme de ses fils, il suffit alors de parcourir l'arbre des feuilles vers la racine pour obtenir ce nombre de modes. La dernière étape consiste à sélectionner les noeuds comportant des signaux monocomposantes de meilleure résolution temporelle. Il s'agit des noeuds à 0 ou 1 ayant un père supérieur ou égal à 2. Cette dernière étape est représentée par des losanges entourant les noeuds sélectionnés.

5.3 Algorithme de sélection d'une meilleure base pour le tatouage

5.3.1 Objectifs de la méthode

Nous avons présenté dans la première partie de ce rapport les définitions et contraintes inhérentes à une méthode de tatouage d'images pour la protection du copyright. Une étude bibliographique a permis de distinguer deux types de méthodes, les tatouages additifs et les tatouages virtuels. Après avoir étudié les avantages et inconvénients de ces deux ensembles de méthodes, nous avons décidé de construire un algorithme fondé sur les principes du tatouage virtuel. L'idée générale de ce type de tatouage est d'exprimer la marque W en modifiant des caractéristiques de composantes de l'image pointées par la clef K. Pour des raisons de robustesse du schéma, les composantes modifiées doivent être perceptuellement significatives, et bien réparties dans le domaine spatial et fréquentiel de l'image. Elles doivent aussi être présentes en nombre suffisant pour permettre l'insertion d'une marque de grande taille.

Nous avons choisi, comme composantes de l'image les coefficients de paquets d'ondelettes. La caractéristique correspondante est la présence de ces paquets dans une base dont nous modifierons la structure pour exprimer la marque. Nous allons maintenant expliquer les motivations de ces choix.

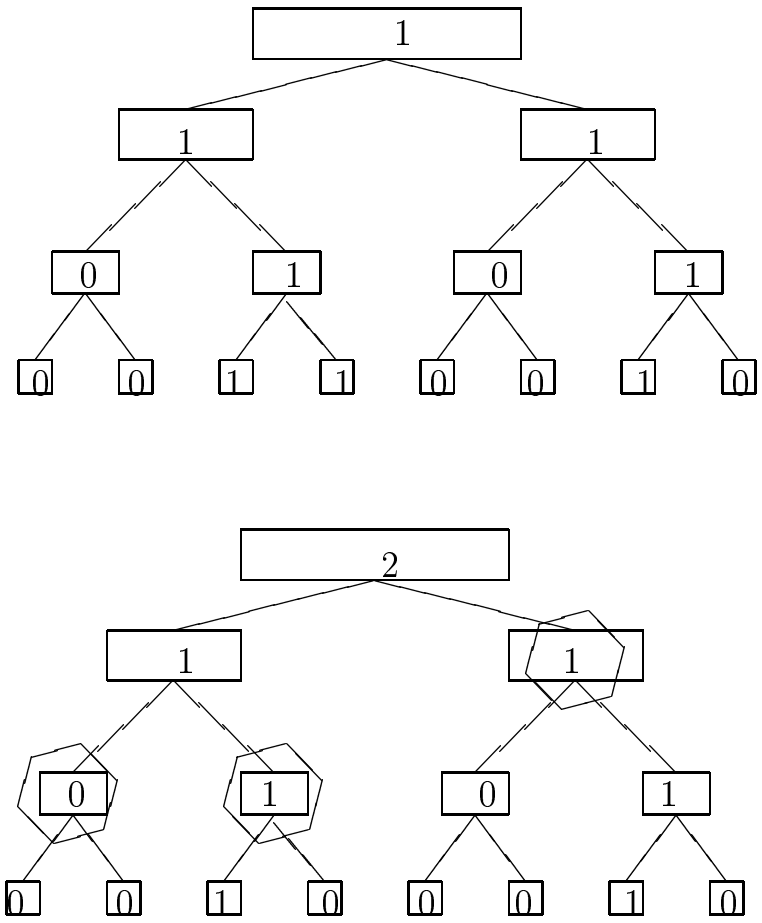


FIG. 5.7 – Étapes de la sélection d'une meilleure base pour la détection de ruptures fréquentielles. La meilleure base obtenue est représentée par des losanges

5.3.2 Principes de la méthode

5.3.2.1 Choix du domaine transformé

Les coefficients d'un paquet d'ondelettes correspondent à la contribution dans l'image de composantes fréquentielles prises à une certaine résolution. Dans un noeud donné, les coefficients représentent donc le comportement de toute l'image à la résolution et dans la bande de fréquence fixée par le noeud. Modifier un paquet d'ondelettes nous assurera donc la répartition de l'information de la marque sur toute l'image. La répartition fréquentielle des modifications se fera naturellement en sélectionnant plusieurs paquets. Une contrainte issue de la robustesse du schéma impose que les composantes choisies pour porter la marque doivent être perceptuellement significatives, ce qui signifie, pour notre méthode, que la construction de la base doit être motivée par ce critère : la meilleure base doit être composée de paquets représentant des contributions significatives de l'image. La dernière contrainte rappelée ci-dessus nous incite à construire une base possédant une structure riche, nous permettant d'obtenir un grand nombre de paquets.

5.3.2.2 Choix de la méthode de modification

Il y a plusieurs façons de modifier les coefficients en paquets d'ondelettes. L'une d'elles consiste à ajouter un bruit à chacun des paquets. Ceci correspond à une méthode de tatouage additive. Si l'on veut utiliser une méthode virtuelle, plusieurs stratégies sont possibles. On peut par exemple comparer les coefficients des paquets entre eux en utilisant une méthode similaire à celle exposée au paragraphe 2.2.3.

On peut aussi envisager de modifier les paquets dans leur globalité en comparant par exemple leur énergie à un seuil. Cette approche possède l'avantage d'utiliser le caractère de décomposition de l'image en bandes fréquentielles.
Prenons un exemple concret : on décide d'augmenter l'énergie du paquet (p, i, j) d'une certaine bande de fréquence (i, j) à la résolution p. On augmente alors l'énergie de ce paquet. Comme on utilise une décomposition en bancs de filtres, si la résolution spatiale n'est pas nulle (p n'est pas maximum), les modifications vont se répartir sur toute l'image adaptativement selon le comportement spatial des coefficients. Cela revient grossièrement à faire une modification sur le spectre de l'image puis à moduler cette modification selon le comportement spatial de la fréquence modifiée, ce qui est très couramment utilisé en tatouage d'images et de sons. Cette méthode nous incite à choisir une base selon un critère énergétique. Nous détaillerons plus précisément les étapes du tatouage dans la troisième partie de ce rapport : l'idée de base du processus de tatouage proposé est d'exprimer la marque en contraignant l'appartenance des noeuds à la meilleure base. Une contrainte fondamentale est donc la stabilité de la base modifiée. La structure de la base doit rester invariante après une attaque quelconque. Cette contrainte est très importante et doit être considérée lors de la construction du critère de sélection de la meilleure base.

5.3.2.3 Choix du critère de sélection de la meilleure base

Contraintes sur les paquets sélectionnés Nous avons vu au paragraphe précédent que les paquets d'ondelettes qui sont pointés par la clef K doivent être des composantes significatives de l'image. Nous les choisirons d'énergie supérieure à un seuil. Il est évident que le nombre de ces paquets imposera directement la longueur de la marque. La meilleure base doit être ainsi constituée d'un nombre maximum de paquets de grande énergie.

La contrainte de stabilité de la base renforce encore ce point de vue. En effet, la présence de paquets de petite énergie (ou contenant peu d'informations) dans la base peut fragiliser sa structure.
Considérons le cas suivant : la meilleure base MB sélectionne dans deux bandes de fréquences voisines un paquet P_E d'énergie significative et un paquet p_e de petite énergie. Après une attaque, les énergies de ces deux paquets peuvent se mélanger : l'énergie d'une composante de P_E en limite de bande se répartit entre les deux paquets ou même devient composante de p_e. Quel que soit le critère choisi, une telle modification du comportement fréquentiel de l'image aura des influences sur la structure de la base : L'information ne sera plus répartie de la même manière entre les deux sous bandes, la base sera modifiée. La seule solution possible permettant d'éviter une telle instabilité de la structure de la base est d'imposer que tous les paquets d'ondelettes sélectionnés soient d'énergie significative.

Choix du critère de sélection On veut donc obtenir une base qui permette de représenter l'image par un ensemble de coefficients significatifs. Chaque noeud sélectionné portera une part significative de l'énergie de l'image. Contrairement aux autres méthodes, on ne cherche pas à séparer l'information contenue dans l'image pour la décorréler (dans le cas de la compression) ou l'analyser (dans le cas de la détection de rupture). On cherche une partition de l'image en coefficients représentatifs : plusieurs composantes fréquentielles peuvent être présentes dans le même noeud, la seule interdiction que l'on impose sur la structure de la base est qu'on ne doit pas sélectionner de noeuds de trop basse énergie.

Le critère entropique permet de sélectionner une base qui optimise la concentration du signal sur quelques coefficients. Dans ce cas, l'image sera exprimée en fonction de peu de coefficients, chaque composante sera finement analysée. Cette analyse très fine de la répartition de l'information sur les paquets d'ondelettes peut conduire à sélectionner une base où l'énergie de l'image est dispersée entre les paquets. On n'aura pas accès aux paquets de grande énergie et de plus la multitude de paquets contenant peu d'information fragilisera la structure de la base.

L'algorithme de sélection de la meilleure base que nous proposons est fondé sur un critère énergétique proche de celui étudié au paragraphe 5.2.3. Nous sélectionnerons les paquets dont l'énergie est supérieure à un seuil et dont l'un des fils est d'énergie inférieure. Comme on le verra ci-dessous, ceci nous permet d'obtenir un nombre maximum de noeuds d'énergie significative. Cette sélection est détaillée au chapitre suivant.

5.3.3 Algorithme

La sélection de la meilleure base est illustrée par la figure 5.8. Elle est constituée de trois étapes. Par souci de simplicité, nous donnons ici les explications et les schémas pour un signal à une dimension.

- La première étape consiste à calculer l'arbre énergétique de la décomposition en paquets d'ondelettes : chaque feuille (j, m) de l'arbre a pour valeur le carré de l'énergie $E_{j,m}$ présente dans le paquet correspondant :

$$E_{j,m} = \|C_{j,m}\|^2 \tag{5.5}$$

- La deuxième étape consiste à sélectionner les noeuds significatifs : on initialise à 1 les noeuds d'énergie supérieure à un seuil s, les autres noeuds sont mis à zéros. Dans l'exemple, le seuil s est pris à $s = 5$.
- La troisième étape consiste à sélectionner la meilleure base : On parcourt l'arbre de la racine vers les feuilles et on sélectionne les noeuds à 1 dont un fils au moins est à zéro. Cette façon de parcourir en prenant pour base initiale la racine puis en comparant les noeuds fils et pères garantit que l'on sélectionne une partition qui forme une base.

On obtient donc une base de décomposition de l'image dans laquelle chaque paquet contient une énergie au moins supérieure au seuil et qui est de profondeur maximale : c'est à dire qu'on dispose du nombre maximum de paquets.

5.3.3.1 Formalisme

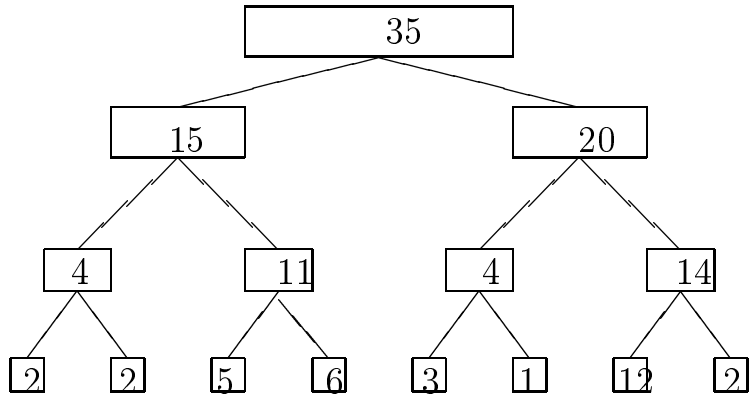
On peut formaliser les étapes de sélection de la meilleure base. Dans notre méthode, un noeud $N_{p,i}$ appartient à la base si et seulement si :

$$N_{p,i} \in \mathcal{F}_s \quad \text{et} \quad N_{p+1,2i} \notin \mathcal{F}_s \quad \text{ou} \quad N_{p+1,2i+1} \notin \mathcal{F}_s \tag{5.6}$$

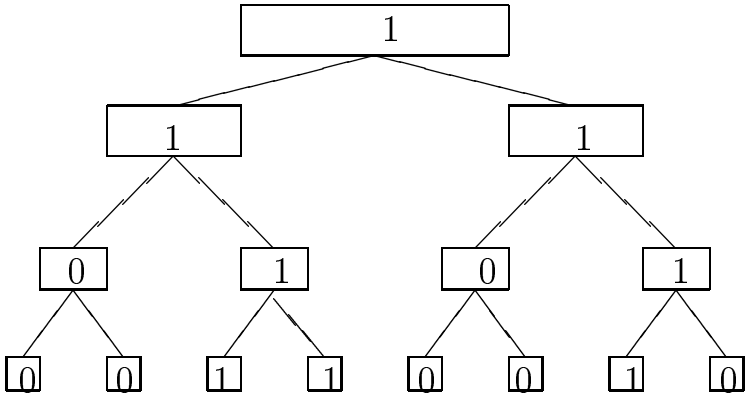
C'est à dire que le noeud est sélectionné s'il appartient à une famille $\mathcal{F}_s$ de noeuds et si l'un de ses fils ne lui appartient pas. $\mathcal{F}_s$ représente la famille de noeuds d'énergie supérieure au seuil s, dont les antécédents sont tous supérieurs à s, ce que l'on peut aussi exprimer de façon redondante par :

$$\begin{aligned}\mathcal{F}_s = \{N_{d,x} \mid \forall(\delta_1) \in \{0,1\},\\ \sum_k |C_{d,x+\delta_1 r_1}(k)|^2 \geq s,\\ r1 = 1 - 2 * (x \text{ modulo}(2)),\\ N_{d-1,E(x/2)} \in \mathcal{F}_s\}\end{aligned}$$

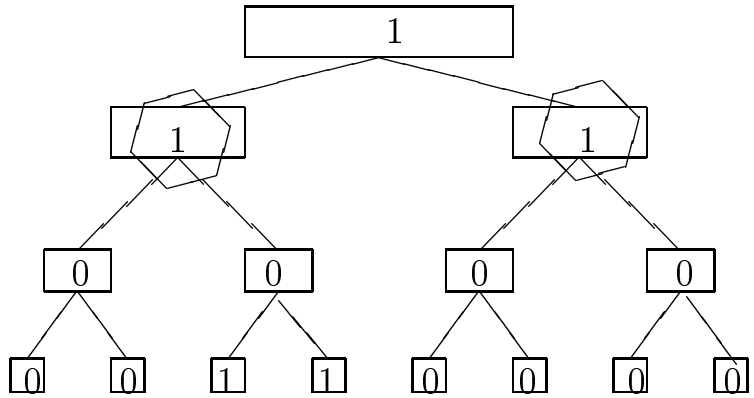
Un noeud appartient à cette famille si son énergie ainsi que celle de son frère sont supérieures au seuil. On impose de plus que le père de ces noeuds est dans $\mathcal{F}_s$, afin de ne pas sélectionner de noeuds de petite énergie.



a- Arbre énergétique



b- Arbre seuillé



c-Meilleure base

FIG. 5.8 – Étapes de la sélection d'une meilleure base pour la détection de ruptures fréquentielles. La meilleure base obtenue est représentée par des losanges

5.3.3.2 Paramètres

Les performances de notre méthode de tatouage seront analysées en terme d'invisibilité et de robustesse aux attaques. Nous détaillerons l'étape de modification dans la prochaine partie. Concernant l'algorithme de sélection de la meilleure base, les paramètres dont dépend la méthode sont :

- le choix de l'ondelette analysante
- le choix du seuil de sélection de la meilleure base.

Nous présenterons au chapitre 10 une étude permettant d'optimiser le choix du seuil en fonction de critères de robustesse.

L'ondelette choisie est celle de Coifman[2]. On diminue ainsi les erreurs dues à la projection de l'image sur l'ensemble V_0 et on privilégie la résolution temporelle. Des tests ont montré que l'utilisation des ondelettes de Daubechies de différentes longueurs donne de moins bons résultats en termes de stabilité de la meilleure base.

5.3.3.3 Exemples de meilleure base

La figure 5.9 b présente la meilleure base obtenue pour l'image «bateau» présentée figure 5.9(a). Dans cet exemple, on a limité la décomposition de l'image en paquets d'ondelettes à la profondeur $p = 4$ de l'arbre de décomposition. On peut observer la répartition de l'énergie dans l'image : au premier niveau de la décomposition, toutes les composantes sont représentées, au second niveau les composantes diagonales ne sont plus détaillées. Au troisième niveau, les composantes verticales diagonales sont détaillées. La figure 5.9(c) montre la répartition de l'énergie des coefficients en paquets d'ondelettes sur cette base.

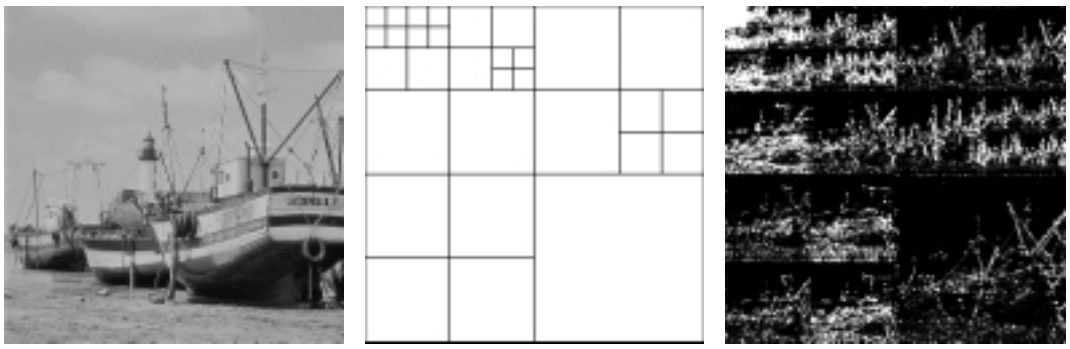


FIG. 5.9 – Image bateau, meilleure base associée et répartition de l'énergie des paquets d'ondelettes dans cette base.

La figure 5.10 présente l'image «BoxWithCross», la meilleure base sélectionnée par le critère et la répartition de l'énergie sur les paquets. On retrouve bien la géométrie de l'image sur la structure de la base, les composantes diagonales sont en particulier plus finement analysées.

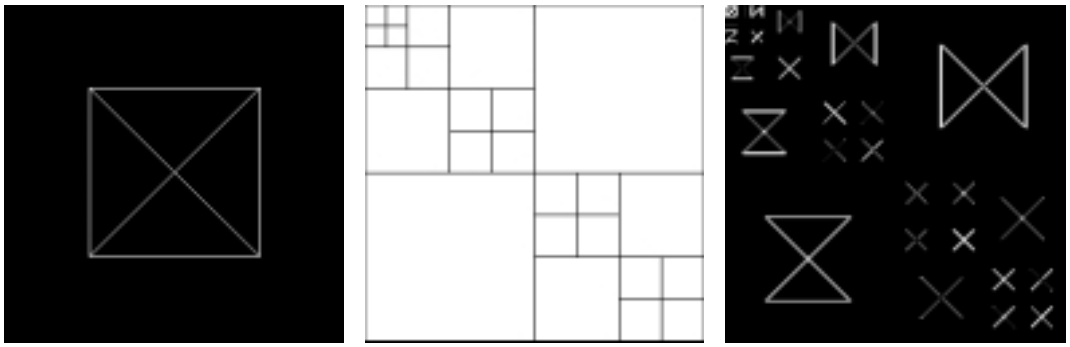


FIG. 5.10 – Image «BoxWithCross», meilleure base associée et répartition de l'énergie des paquets d'ondelettes dans cette base.

Troisième partie

Présentation de l'algorithme de tatouage d'images par paquets d'ondelettes

Chapitre 6

L'Algorithme de tatouage d'images par paquets d'ondelettes

La meilleure base obtenue par l'application de l'algorithme exposé dans le chapitre précédent est constituée de paquets représentant des composantes significatives de l'image. Le principe de la méthode de tatouage que nous présentons dans cette partie consiste à modifier l'énergie de ces paquets afin d'imposer à la base une structure fixée par la watermarque.

Dans ce chapitre [1], nous allons détailler les différentes étapes du processus de tatouage d'images. Nous commencerons par donner un exemple simple permettant d'illustrer le principe de modification de la structure de la base. Nous détaillerons ensuite les étapes d'implémentation et de détection de la marque de façon conceptuelle et schématique.

Dans le chapitre suivant, nous présenterons un exemple simple de l'application de notre processus à une image test. Nous donnerons ensuite quelques résultats de tatouage d'images.

6.1 Exemple d'introduction

6.1.1 Implémentation de la marque

Le schéma de la figure 6.1 représente un exemple simple de modification de la meilleure base par tatouage. La première partie de la figure représente l'arbre de décomposition en paquets d'ondelettes. Pour simplifier le schéma, nous avons représenté le cas d'un signal d'une dimension (l'arbre est alors binaire)[2]. La meilleure base B obtenue avec le critère énergétique, est constituée des noeuds entourés par des carrés. Une clef privée K sélectionne deux noeuds de cette base (indiqués par des ronds sur la figure). L'algorithme de marquage consiste à modifier l'image de façon à ce que la meilleure base de la nouvelle image ne contienne plus ce couple de noeuds lorsque la marque vaut «1».

[1] L'algorithme proposé dans ce chapitre a été présenté et publié lors de la conférence GRETSI [56].

[2] Nous présenterons un exemple en deux dimensions au paragraphe 7.1.

La deuxième partie du schéma représente l'arbre de décomposition et la meilleure base B^* une fois que les modifications ont eu lieu. La structure de la meilleure base a changée : la répartition des noeuds la constituant (ils sont entourés par des carrés) a changé. Si l'on regarde les noeuds pointés par K (entourés par des ronds), l'un des deux noeuds n'est plus dans la meilleure base. Il y a eu une modification de ce noeud ce qui signifie que la marque implantée est le bit «1». Si l'on avait voulu implanter le bit «0», il n'y aurait pas eu de modification. C'est cette modification de la structure de la meilleure base qui est le principe de notre méthode. On peut noter que l'on remplace le noeud modifié par ses fils dans la nouvelle base, on a ainsi une base de paquets d'ondelettes.

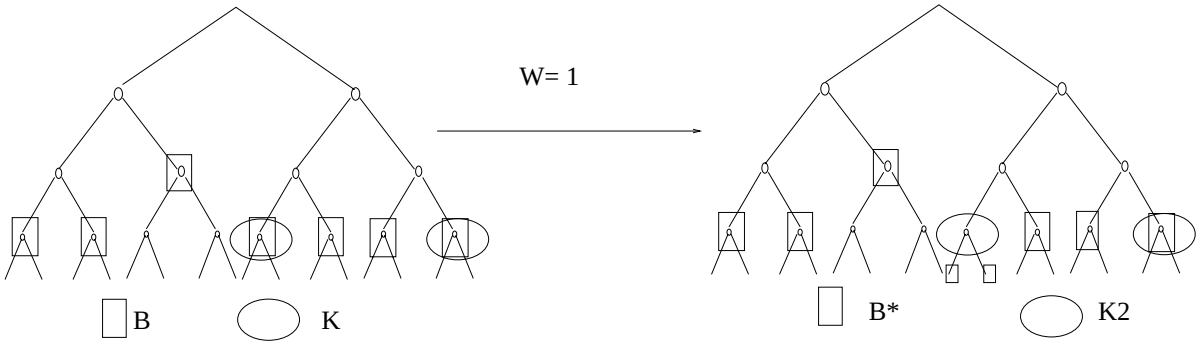


FIG. 6.1 – Modifications de la structure de la meilleure base par tatouage.

6.1.2 Détection de la marque

La figure 6.2 présente l'étape de détection de la marque. On calcule la meilleure base B' de l'image que l'on souhaite tester. L'arbre de décomposition est représenté pour un signal d'une dimension. La meilleure base est constituée des noeuds entourés par des carrés. La clef privée K sélectionne deux noeuds de l'arbre. L'un des noeuds pointé par K n'appartient pas à la base B'. On en déduit qu'il y a eu une modification, la marque lue est le bit «1».

6.2 Le processus d'implémentation de la marque

6.2.1 Schéma du Processus

Le schéma général d'implantation de la marque est représenté figure 6.3. L'image hôte I est tatouée d'une marque W, grâce à un code propriétaire C. Les sorties de ce processus sont l'image résultante I^* et la clef de détection K. Les étapes constituant le processus d'implémentation sont détaillées ci-dessous :

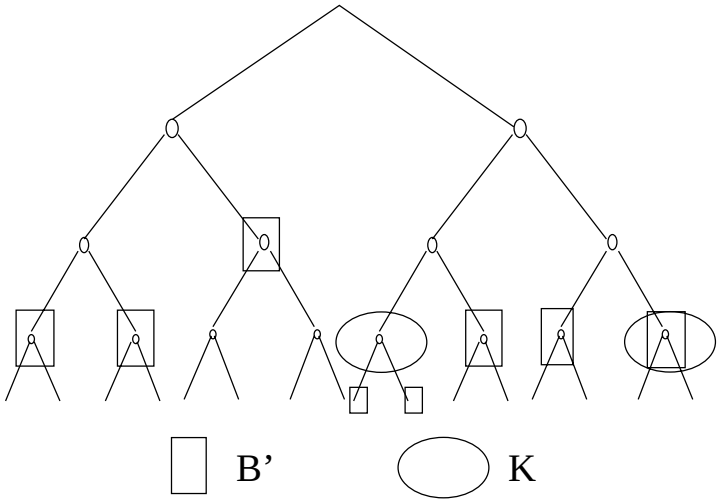


FIG. 6.2 – Lecture du code à la détection

- La première étape est la sélection de la meilleure base B de décomposition de l'image en paquets d'ondelettes. On utilise l'algorithme présenté au paragraphe 5.3 permettant de sélectionner le nombre maximum de paquets d'énergie significatives.
- L'étape «1*bis*» permet de construire la clef privée de détection. Cette clef est constituée d'une famille de pointeurs sur les noeuds de la base, elle dépend de la structure de la base et d'un code propriétaire C.
- L'étape 2 est la sélection de sous-ensembles de B par K et la modification de ces sous-ensembles selon les valeurs de la marque W. C'est l'étape d'encodage de la marque par modification de la structure de la base B. On obtient une base modifiée B^*.
- L'étape 3 est la reconstruction de l'image.

Nous allons détailler les étapes 1*bis* et 2 de ce processus, les étapes 1 et 3 étant décrites au paragraphe 5.3.

Notations Les notations présentées dans le tableau 6.1 nous serviront dans l'ensemble de ce chapitre.

6.2.2 La construction de la clef privée de détection

La clef K sélectionne l'ensemble des noeuds de la meilleure base qui porteront la marque. Elle est composée d'un ensemble de couples de pointeurs sur les noeuds de la base :

$$K = \{(K_i(1), K_i(2))\}_{i=[1..m]} \tag{6.1}$$

Chaque couple de la clef définit un sous-ensemble B_i à deux éléments de B que nous appellerons sous-base. Chaque B_i est donc composée de deux noeuds. Chaque sous-base portera un bit de la marque, le nombre m de sous-bases est donc la longueur de la marque W.

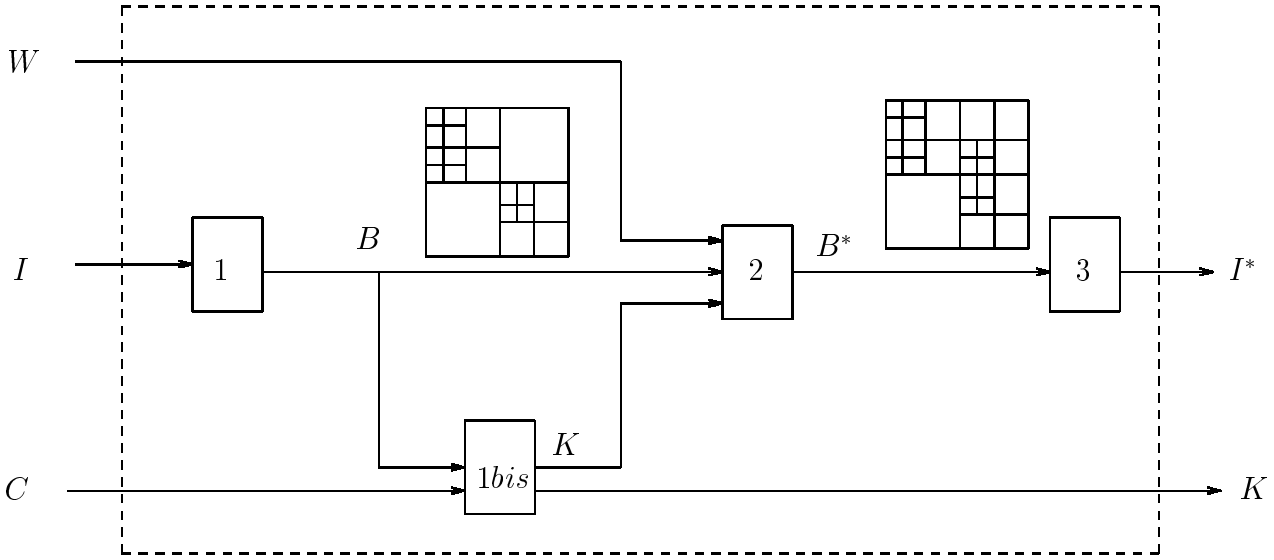


FIG. 6.3 – Schéma d'implémentation d'une marque

La clef K est obtenue à partir de la meilleure base B et d'un code utilisateur C qui permet d'obtenir des clefs différentes pour des propriétaires différents. Le nombre de code C possible dépend du nombre de noeuds présents dans la meilleure base. Chaque C représente une façon d'obtenir m sous-ensembles de cardinal 2 parmi un ensemble B de cardinal fixé égal à N_B (N_B est le nombre de noeuds présents dans la meilleure base). Par souci de simplicité, nous avons choisi de travailler sur des sous-bases disjointes ce qui correspond à un tirage sans remise. Le cardinal de l'ensemble $\mathcal{C}$ de tous les codes C possibles pour une base B est alors de :

$$|\mathcal{C}| = (\frac{1}{2})^m \frac{N_B!}{(N_B - 2m)!} \tag{6.2}$$

La clef K est donc obtenue par application d'un opérateur E_B sur l'espace $\mathcal{C}$ dans l'espace des clef $\mathcal{K}$.

$$\begin{array}{ccc} \mathcal{C} & \longmapsto & \mathcal{K} \\ C & \longmapsto & K \end{array} \tag{6.3}$$

Remarques

La confidentialité de la clef K repose d'une part sur celle de la base et d'autre part sur celle du code C. Plus $|\mathcal{C}|$ est grand, plus la clef sera difficile à estimer par un pirate. Une étude sur une attaque intentionnelle consistant à enlever la marque en estimant la clef sera étudiée au paragraphe 13.2.4.

La clef que nous présentons ici possède une structure simple qui peut être étendue. Par exemple, on peut utiliser une clef composée de m p-uplets, on peut aussi prendre des sous-bases d'intersection non vide. Une étude portant sur les extensions possible de

TAB. 6.1 – Notations

notations	objets
I	image originale
I^*	image tatouée
B	meilleure base
B^*	meilleure base tatouée
C	code utilisateur
K	clef privée de détection
W	watermarque
m	longueur de la watermarque
s	seuil de sélection de la meilleure base
N_B	nombre de noeuds de B
B_i	couple de noeuds de B, *sous-base*
p_i	cardinal de B_i
B_i^*	sous-base tatouée
SB	ensemble des m sous-bases
SB^*	ensemble des m sous-bases tatouées
$N_{p,i,j}$	noeud de l'arbre de décomposition
$C_l(k)$	coefficient en paquets d'ondelettes du noeud N_l

la clef K et leurs implications sur la méthode de tatouage sera présentée au paragraphe 14.

L'opérateur E choisit les noeuds de la base à partir de C sans prendre en compte leurs caractéristiques (valeur de l'énergie, niveau de résolution, bande de fréquence occupée). Nous étudierons les influences de ces paramètres au chapitre 8.

6.2.3 Les modifications de la structure de la meilleure base

Une fois la clef K construite, les sous-bases B_i sont sélectionnées. Chaque sous-base va porter un bit de la marque. La watermarque W est un code binaire de longueur m :

$$W = \{W_i\}_{i=(1..m]},\ W_i \in \{0,1\} \tag{6.4}$$

Chaque bit de la marque est associé à une sous base et représente le nombre de modifications que l'on fait dans la sous-base correspondante. Dans notre cas, il y aura donc 0 ou 1 modification dans chaque B_i. Comme on l'a explicité au paragraphe 5.3, modifier une sous base consiste à exclure l'un des noeuds pointés par K_i de sa structure et de le remplacer par ses fils. Les différentes étapes de cette modification sont détaillées ci-dessous.

6.2.3.1 Les différentes étapes de la modification

La modification de la structure de la meilleure base à lieu en trois phases :

- Les sous-bases B_i sont sélectionnées par K. On peut noter $B_i = K_i(B)$. Ce sont des couples de noeuds de B.
- Pour chaque B_i, le bit i de la marque est exprimé de la façon suivante :
  - Si $W_i = 0$, il n'y a pas de modifications : $B_i^* = B_i$
  - Si $W_i = 1$, on fait une modification : B_i devient B_i^*, cette nouvelle base ne contenant plus qu'un paquet pointé par K_i. Le paquet disparu est remplacé dans la structure de B_i^* par ses quatre fils.
- Chaque sous-base B_i^* remplace B_i dans la meilleure base B.

6.2.3.2 Illustration

La figure 6.4 illustre l'étape de modifications des sous-bases. Pour simplifier le schéma, nous avons représenté cette étape sur un arbre binaire (c'est à dire pour un signal d'une dimension).
La première partie de la figure présente l'arbre de décomposition du signal en paquets d'ondelettes. Les noeuds constituant la meilleure base B sont indiqués par des carrés. La clef K est composée de deux couples de pointeurs $K1$ et $K2$ et sélectionne les noeuds de la base représentés respectivement par des losanges (pour la sous-base B_1) et des ronds (pour B_2).
La watermarque est le vecteur $W = (0, 1)$. On ne modifiera donc pas la sous-base B_1 et on fera une modification sur B_2.
La deuxième partie de la figure représente la nouvelle meilleure base B^* une fois que la modification a été faite. Un des noeuds pointés par $K2$ à disparu de la structure de la base et a été remplacé par ses fils. On a ainsi modifié la structure de la base afin de coder la watermarque.

Notons $V_K(\hat{B})$ le p-uplet $(V_1, V_2, .., V_m)$ où V_i est le nombre de noeuds pointés par K_i qui ne sont pas dans une base donnée $\hat{B}$. Dans l'application présentée ici $m = 2$ et $V_i = 0$ ou 1. De plus, $V_K(B) = (0, 0)$ car on choisit de toujours pointer par K des éléments de B. Après modification, on a dans notre exemple, $V_K(B^*) = (0, 1) = W$

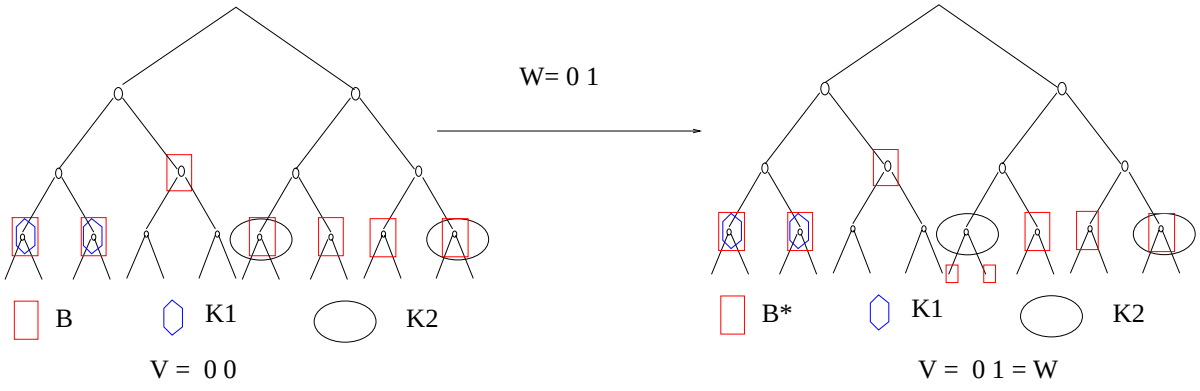


FIG. 6.4 – Modifications de la structure de la meilleure base par tatouage.

6.2.3.3 Remarque

On choisit de supprimer un noeud en le remplaçant par ses fils. Cette méthode permet d'une part de conserver une structure de base et d'autre part de ne pas influer sur les autres noeuds sélectionnés par la base. En effet, si l'on remplaçait le noeud exclu par son père, tous les noeuds de la base appartenant au sous arbre de racine le père seraient eux aussi supprimés.

6.2.3.4 Formalisme

De part sa qualité de pointeur, la clef K sélectionne m couples de noeuds de B, notés SB :

$$K(B) = SB = \{B_i\}_{i\in[1..m]} \tag{6.5}$$

On a la relation suivante :

$$B = SB \oplus BS = \oplus\{B_i\} \oplus BS \tag{6.6}$$

où BS est le complémentaire de SB dans B.
La modification des sous-bases est un opérateur $\mathcal{O}$ de l'espace des parties de B et de l'espace des watermarques $\mathcal{W}$ dans l'espace des parties de B^* :

$$\begin{array}{ccc} \mathcal{P}(B) \times \mathcal{W} & \longmapsto & \mathcal{P}(B^*) \\ (SB, W) & \longmapsto & SB^* = B_1^*, B_2^*, ..., B_m^* \end{array} \tag{6.7}$$

B^* est construite par

$$B^* = SB^* \oplus BS = \oplus\{B_i^*\} \oplus BS \tag{6.8}$$

cette dernière relation justifie le fait que l'on appelle sous-bases les B_i ou B_i^*.
La marque est exprimée de la façon suivante

$$W_i = |K_i(B)| - |K_i(B^*)| \tag{6.9}$$

W est le nombre de noeuds présents dans B et pointés par K qui ont disparu dans B^*. Pour nous,

$$W_i = 2 - |K_i(B^*)| = |K_i(B^*)| \text{ modulo}(2) \tag{6.10}$$

6.2.3.5 Obtention de la meilleure base modifiée

La structure de la base a été modifiée selon les étapes détaillées ci dessus. Pour pouvoir détecter la marque, il est évident que l'on doit retrouver la base B^*, c'est à dire que B^* doit être la **meilleure base** de l'image tatouée pour notre critère.

Les modifications de la structure de B se font en remplaçant certains noeuds de B par leurs quatre fils. Pour notre critère, cela signifie que de l'énergie à été rajoutée aux fils. Nous avons vu en effet que le critère de sélection de la meilleure base était le suivant : Un noeud N_p sera sélectionné si N_p, ses frères et ses antécédents sont d'énergie supérieure à un seuil s et si l'énergie de l'un de ses fils ne l'est pas.

Pour faire de B^* la meilleure base au sens de notre critère, il suffit d'augmenter suffisamment l'énergie des paquets fils des paquets exclus de la structure. Nous allons voir au paragraphe suivant le détail de la modification de l'énergie des coefficients des paquets fils.

Remarque Il peut arriver que ces modifications entraînent la sélection des petits fils du noeud modifié. Cela n'a aucun impact sur notre méthode puisque l'information que l'on transmet est l'absence du noeud (et non la présence de ses fils).

6.2.3.6 La modification des coefficients en paquets d'ondelettes

Notre objectif est d'ajouter de l'énergie à certains coefficients en paquets d'ondelettes. Notons $C_i(k)$ ces coefficients, i étant un multi-indice représentant le niveau de résolution et la bande fréquentielle dans lesquels se trouve ce paquet et k étant le bi-indice de translation spatiale. La solution que nous proposons consiste à augmenter le gain en énergie du paquet i selon :

$$C_i^*(k) = \alpha_i C_i(k) \tag{6.11}$$

avec

$$\alpha_i = \sqrt{\frac{s}{\|C_i\|_2^2}} \tag{6.12}$$

Cette façon d'augmenter l'énergie du paquets d'ondelettes a plusieurs avantages :
- On n'ajoute pas de nouvelles composantes fréquentielles qui perturberait la structure de la base.
- On prend en compte l'information spatiale présente dans le paquet : la valeur du coefficient $C_i(k_0)$ est augmentée selon son amplitude.
- On minimise la distorsion (au sens des moindres carrés) entre l'image originale et l'image tatouée. La démonstration de cette propriété est donnée au paragraphe 13.1.

Si l'on prend la valeur de gain α_i proposé dans l'équation 6.12, l'énergie des nouveaux paquets est égale au seuil s. A la moindre diminution de cette énergie, le paquet ne sera pas sélectionné dans la meilleure base. La structure de la base ne sera alors plus modifiée, le bit de la marque transmise sera faux. Pour remédier à ce problème, nous introduisons un paramètre ε de **force** du tatouage :

$$\alpha_i = \sqrt{\frac{s+\varepsilon}{\|C_i\|_2^2}} \tag{6.13}$$

Ce paramètre de force influera sur la qualité du tatouage et sur sa robustesse. Une étude présentée au paragraphe 11 permettra d'optimiser la valeur de ε pour chaque paquet selon un critère psychovisuel.

6.2.3.7 Choix de la nouvelle base

Nous avons vu que le principe des modifications structurelles des sous-bases nous laisse le choix du noeud que l'on va modifier. En effet, une sous-base est composée de deux noeuds et subira au plus une modification. Cette liberté dans le choix du paquet nous permet de limiter le nombre de cas où nous rajoutons du «bruit» dans l'image en augmentant l'énergie des coefficients.

Appelons N_p un paquet de la base B que l'on veut remplacer par ses fils N_{pf}. Nous savons que N_p est un paquet contenant une information représentative de l'image mais nous ne connaissons pas la répartition de l'information entre les paquets fils. Il est par exemple possible que les composantes significatives présentes dans N_p se répartissent sur trois des fils, le dernier ne contenant que du bruit. Modifier N_p augmenterait alors le gain du bruit.

Pour éviter cela, on choisit parmi les deux noeuds possibles appartenant à une sous-base, celui dont l'énergie des fils est la mieux répartie. En d'autres termes, on choisit le noeud de plus forte entropie.

De plus, cette liberté dans le choix de la modification nous assurera une meilleure robustesse à des attaques intentionnelles. En effet, nous verrons au paragraphe 13.2.4 que ce choix complique les attaques consistant à inverser la marque.

6.2.3.8 Conclusion

Dans ce paragraphe, nous avons présenté l'étape de modification de la structure de la base. Par souci de simplicité, nous avons considéré des sous-bases à deux éléments et une marque binaire, il est évident que l'on peut généraliser le propos. Ces paramètres sont les conséquences directes des choix que nous avons fait à l'étape de la construction de la clef. Nous présenterons au paragraphe 14 les extensions possible de la méthode.

Nous avons présenté les étapes du processus d'implémentation de la marque. Nous allons maintenant décrire le processus de détection semi-privé de la marque.

6.3 Le processus de détection de la marque

6.3.1 Principe du Processus

Le schéma général de détection de la marque est représenté figure 6.5. Les entrées de ce processus sont la clef secrète de détection K, l'image test I' et la marque recherchée W. La sortie est une variable de décision $y_n \in \{0, 1\}$ indiquant si W est considérée présente dans I' (cas où $y_n = 1$) ou si elle est considérée absente (cas $y_n = 0$). Notre processus fait donc partie des schémas semi-privés. La détection de la marque est composée de trois étapes décrites ci-dessous :

- La première étape est la sélection de la meilleure base B' de décomposition de l'image en paquets d'ondelettes.

- L'étape 2 est la lecture du code W', on regarde parmi les noeuds pointés par la clef K ceux qui sont présents dans la structure de la meilleure base.
- L'étape 3 est la comparaison de la marque extraite W' avec la marque recherchée W. On procède par distance de Hamming puis par seuillage du résultat. Si la distance est inférieure à d la marque est considérée présente.

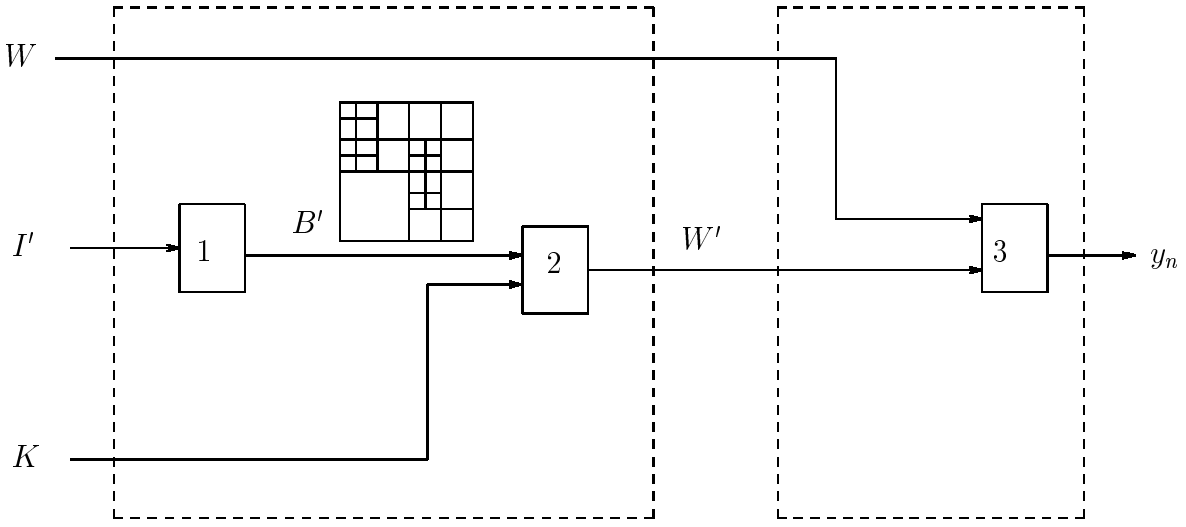


FIG. 6.5 – Schéma de détection de la marque

Le tableau 6.2 donne les notations utilisées dans cette étape.

TAB. 6.2 – Notations

notations	objets
I'	image à tester
B'	meilleure base à tester
K	clé privée de détection
W'	watermarque extrait
W	watermarque original
y_n	coefficient de réponse de la détection

L'étape de détection de la marque étant très simple, nous allons simplement illustrer la deuxième étape consistant à lire la marque.

La figure 6.6 présente la lecture du code. La meilleure base B' de l'image test I' est représentée par des carrés sur l'arbre de décomposition. La clef K est constituée de deux paires de pointeurs. La première paire sélectionne deux noeuds de la base, il y a eu 0 modification et $W'_1 = 0$. Il y a un absent parmi les noeuds pointés par K_2 : $W'_2 = 1$. On

peut remarquer ici que, comme le montre la relation 6.10, on peut compter les noeuds absents ou les présents.

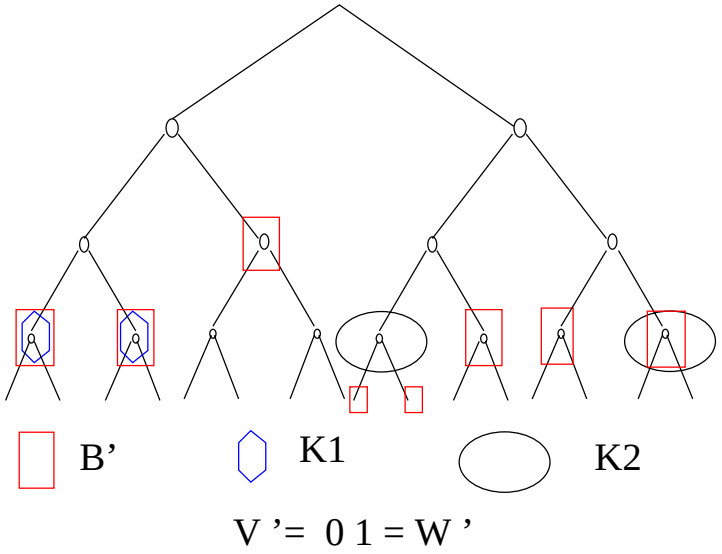


FIG. 6.6 – Lecture du code à la détection

6.4 Conclusion

Nous avons présenté ici l'algorithme de tatouage par paquets d'ondelettes que nous proposons. Il est constitué de deux étapes principales : l'implémentation de la watermarque et sa détection.

L'implémentation est une application $\mathcal{E}$ qui à un code propriétaire C et à une image originale I fait correspondre une image tatouée I^* et une clef de détection K.

$$\begin{array}{ccc} \mathcal{C} \times \mathcal{I} & \longmapsto & \mathcal{K} \times \mathcal{I} \\ (C, I) & \longmapsto & (K, I^*) \end{array} \tag{6.14}$$

Cette étape est fondée sur les algorithmes de tatouages virtuels. Elle consiste à modifier la structure d'une meilleure base de paquets d'ondelettes. Les composantes modifiées sont toutes d'énergie significative. Elles sont caractéristiques du comportement spatio-fréquentiel de l'énergie de l'image. Les modifications des coefficients en paquets d'ondelettes respectent la répartition spatiale de l'énergie et minimisent la distorsion en norme L^2. Une analyse de la méthode sera présentée à la partie V de ce rapport.

L'étape de détection de la marque est semi-privée : c'est une application $\mathcal{D}$ qui à une image test I', à une clef privée K et à la watermarque cherchée W fait correspondre une valeur de décision y_n.

$$\begin{array}{ccc} \mathcal{K} \times \mathcal{I} \times \mathcal{W} & \longmapsto & \{0, 1\} \\ (K, I', W) & \longmapsto & y_n \end{array} \tag{6.15}$$

Cette détection consiste à lire la marque sur la structure de la meilleure base puis à la comparer à la marque recherchée.

Le chapitre suivant présente le déroulement de la méthode de tatouage sur un exemple à deux dimensions puis on montre les premiers résultats sur quatre exemples. Une étude portant sur la robustesse à diverses attaques sera présentée au paragraphe 8. La partie IV présente les améliorations que l'étude de robustesse nous a conduits à faire.

Chapitre 7

Premiers résultats

Dans le chapitre précédent, nous avons présenté l'algorithme de tatouage par paquets d'ondelettes. Nous commencerons ce chapitre par décrire les différentes étapes détaillées précédemment sur un exemple simple de tatouage d'image.

Nous présenterons ensuite les premiers résultats obtenus avec cette méthode. Les paramètres d'entrée de notre processus sont le seuil s de sélection de la meilleure base, la longueur m de la watermarque et le coefficient ε de force du tatouage. Nous allons évaluer ici les performances de la méthode de tatouage en terme d'invisibilité et de robustesse pour des applications correspondant à différents choix sur les paramètres d'entrées du processus.

Ce chapitre est constitué de cinq parties représentant chacune un exemple de tatouage d'image. Le premier exemple est explicatif, nous présentons en détails les étapes du tatouage de l'image «bateau». Les trois exemples suivants donnent un aperçu des résultats du tatouage de cette même image, pour différentes longueurs de marque et différentes valeurs de force. Le dernier exemple montre les résultats que l'on obtient en tatouant l'image «fruit».

7.1 Exemple de tatouage d'image

7.1.1 Implémentation de la marque

La figure 7.1(a) présente l'image originale «bateau» que nous allons tatouer dans cet exemple. La première étape de l'algorithme consiste à calculer la meilleure base B de cette image avec le critère énergétique présenté paragraphe 5.3. Par souci de simplicité on arrête la décomposition au niveau $p = 4$ de l'arbre. La meilleure base est représentée dans la figure 7.1(b), elle est obtenue pour un seuil $s_t = 2.10^{-4}E_t$ où E_t est l'énergie totale de l'image. Dans la suite de ce rapport, on notera s le seuil obtenu pour l'image normalisée, c'est à dire $s = s_t/E_t$.

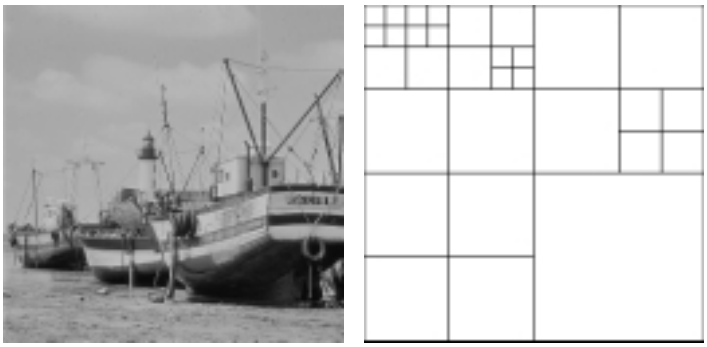


FIG. 7.1 – Image bateau et meilleure base associée

La clef privée détermine l'ensemble des paquets qui porteront l'information permettant d'exprimer la marque. Dans cet exemple, elle est composée de 9 paires de pointeurs sélectionnant 9 couples de noeuds appartenant à la base, c'est à dire 9 sous-bases. La clef choisie est la suivante :

$$\begin{aligned} K = \{&(K_1(1), K_1(2)) \\ &(K_2(1), K_2(2)) \\ &... \\ &(K_9(1), K_9(2))\} \end{aligned}$$

La répartition des noeuds pointés par K est présentée à la figure 7.2. On a indiqué sur la structure de la meilleure base les pointeurs $K_i(j)$ correspondants aux noeuds. Chaque couple de noeuds définissant une sous-base portera un bit d'information imposée par la marque.

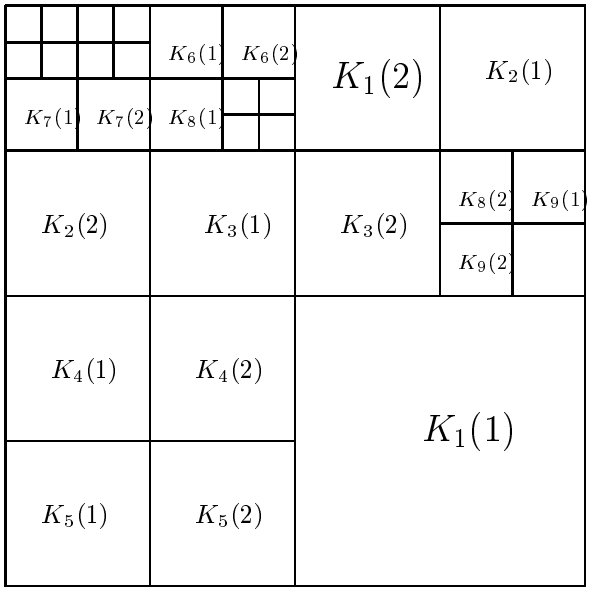


FIG. 7.2 – Répartition des noeuds pointés par la clef sur la meilleure base

La watermarque choisie est le vecteur $W = \{1, 0, 1, 0, 1, 0, 1, 0, 1\}$. Elle indique le nombre de modifications que l'on doit faire sur chaque sous-base.

- Si $W_{j_0} = 1$ on modifie B_{j_0} en supprimant l'un des noeuds la constituant et en le remplaçant par ses fils.
- Si $W_{j_0} = 0$ on ne fait rien.

Dans l'exemple le noeud pointé par $K_1(1)$ est modifié, la nouvelle base contiendra ses quatre fils.
La nouvelle base obtenue pour la clef K et la marque W est représentée à la figure 7.3.

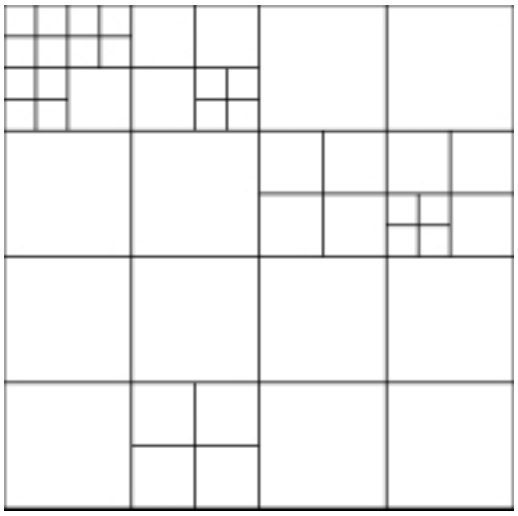


FIG. 7.3 – Base modifiée par tatouage

On reconstruit l'image grâce à l'algorithme de reconstruction parfaite. La figure 7.4 présente les images originale et tatouée. Bien que l'on ne perçoive pas de détériorations, le PSNR est assez faible (34.61dB).

FIG. 7.4 – Images originale et tatouée

L'image de la différence entre les deux images originale et tatouée est présentée dans le domaine spatial sur la figure 7.5. On a amplifié cette différence de façon à rendre visibles les modifications. On peut remarquer que les modifications sont présentes sur les composantes significatives de l'image (les bateaux) et étalées sur l'image. Dans le domaine fréquentiel, cette image différence est représentée figure 7.6. On voit que les modifications (en blanc sur la figure) s'étalent partout sauf dans les très basses fréquences (au centre de la figure).

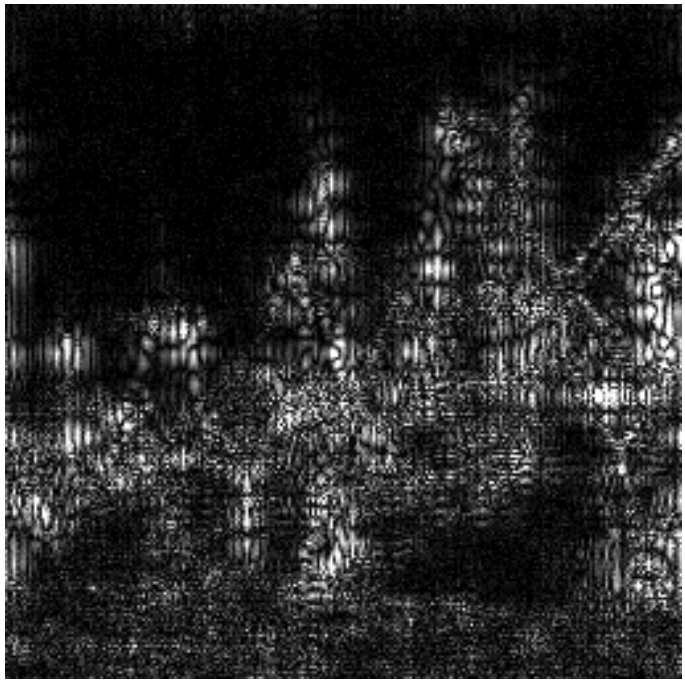


FIG. 7.5 – Image différence des images originale et tatouée

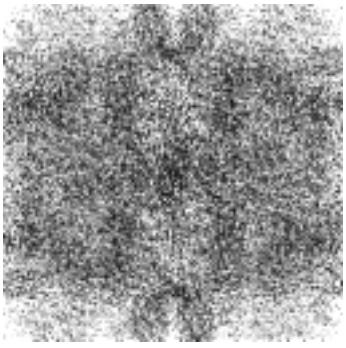


FIG. 7.6 – Spectre de l'image différence des images originale et tatouée

L'image ainsi tatouée est alors distribuée, elle est susceptible de subir des attaques. Le prochain paragraphe présente sur ce même exemple le processus de détection de la

marque.

7.1.2 Détection de la marque

L'image test est l'image tatouée précédemment. Comme dans l'étape d'implémentation, la première étape consiste à calculer la meilleure base, celle ci est présentée figure 7.7.

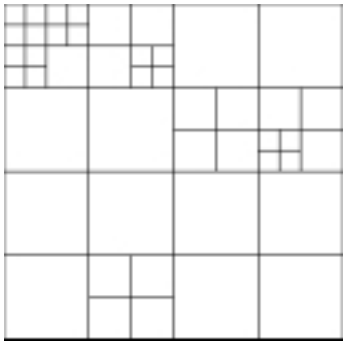


FIG. 7.7 – Meilleure base

La deuxième étape consiste à lire la marque W' : On regarde parmi chaque sous-base B_i pointée par K_i le nombre de noeuds absents. La figure 7.8 représente la meilleure base sur laquelle nous avons indiqué les noeuds pointés par K. Les noeuds absents sont marqués d'un (ø). Le noeud $K_1(1)$ est par exemple absent de la structure de cette base.

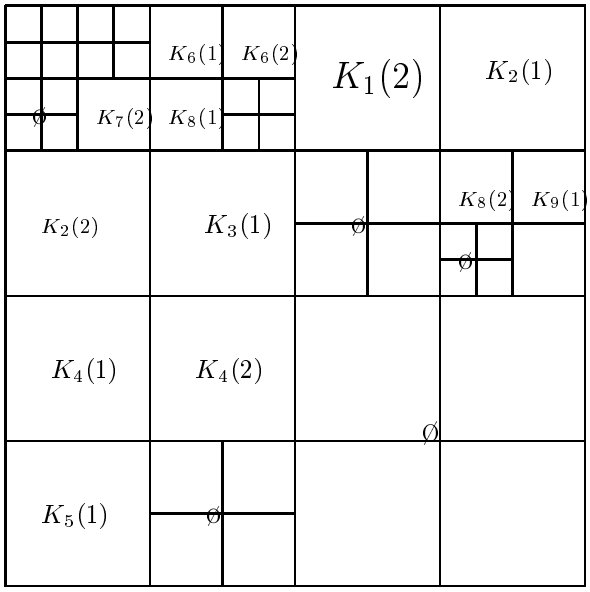


FIG. 7.8 – Meilleure base et répartition des noeuds pointés par K, les noeuds absents sont représentés par «ø»

W' est le nombre de noeuds absents de la base pour chaque couple pointé par la clef. Ici, on retrouve bien $W' = \{1, 0, 1, 0, 1, 0, 1, 0, 1\} = W$

On compare alors la marque extraite avec la marque voulue. On utilise pour cela la distance de Hamming : on calcule la moyenne des valeurs absolues des différences bits à bits entre la marque extraite et la marque voulue, c'est à dire la moyenne des erreurs. Dans notre cas, cette distance est de 0 : la marque a bien été retrouvée.

On peut représenter les performances du détecteur par un graphique, comparant la distance obtenue entre W' et W avec celles obtenues entre W' et une population de marques aléatoires. On applique alors à ces mesures un seuil de décision d, si la valeur de distance entre W et W' est inférieure à d, la marque W sera considérée présente dans l'image.

La figure 7.9 présente les réponses du détecteur à 512 watermarques générées aléatoirement. La watermarque W' apparaît en position 200. Dans notre cas, il n'y a pas de redondance et la marque est courte, le schéma des performances du détecteur n'est pas significatif du bon fonctionnement de la détection (alors que l'on a une détection parfaite).

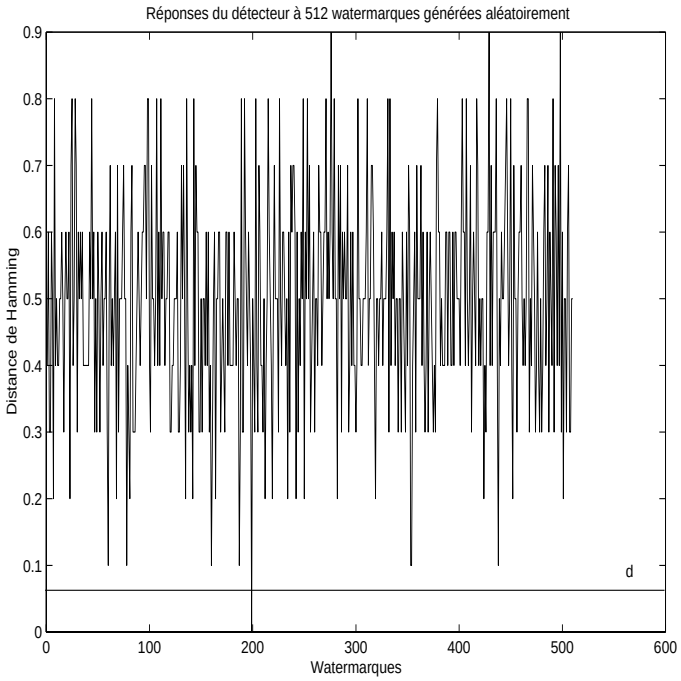


FIG. 7.9 – Réponses du détecteur à 512 watermarques générées aléatoirement, la watermarque voulue est en position 200 des abscisses.

7.2 Premier exemple

7.2.1 Implémentation de la marque

La figure 7.10 présente les résultats que l'on obtient en insérant une watermarque de petite longueur (64 bits) dans l'image bateau de taille 256×256 codée sous 8 bits par pixels. La marque est constituée d'un message binaire de longueur 32 bits assorti d'un coefficient de redondance de 2. Dans la suite de ce rapport, on dira alors que la marque est de longueur 2×32 bits. La clef K est composée des couples de noeuds voisins pour un parcours de la meilleure base de droite à gauche puis de haut en bas (des basses vers les hautes fréquences). Le seuil de sélection de la meilleure base s est pris grand $s = 10^{4.8}$. La force du marquage est prise à $\varepsilon = \frac{s}{10}$. Le PSNR entre les deux images est de 42.09 dB, ce qui est un bon résultat. Il n'y a pas de distorsions visibles entre les deux images.

FIG. 7.10 – Image originale et image marquée

La figure 7.11 présente la différence entre les deux images originale et tatouée. Les niveaux de gris ont été fortement amplifiés, les différences paraissent très petites.

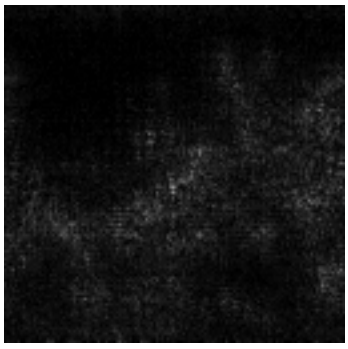


FIG. 7.11 – Image différence des images originale et marquée

La figure 7.12 représente les meilleures bases de l'image originale et de l'image marquée. Le choix du seuil de sélection entraîne la sélection dans la base de noeuds de résolution spatiale moyenne. On voit que les modifications sont étalées sur toutes les fréquences.

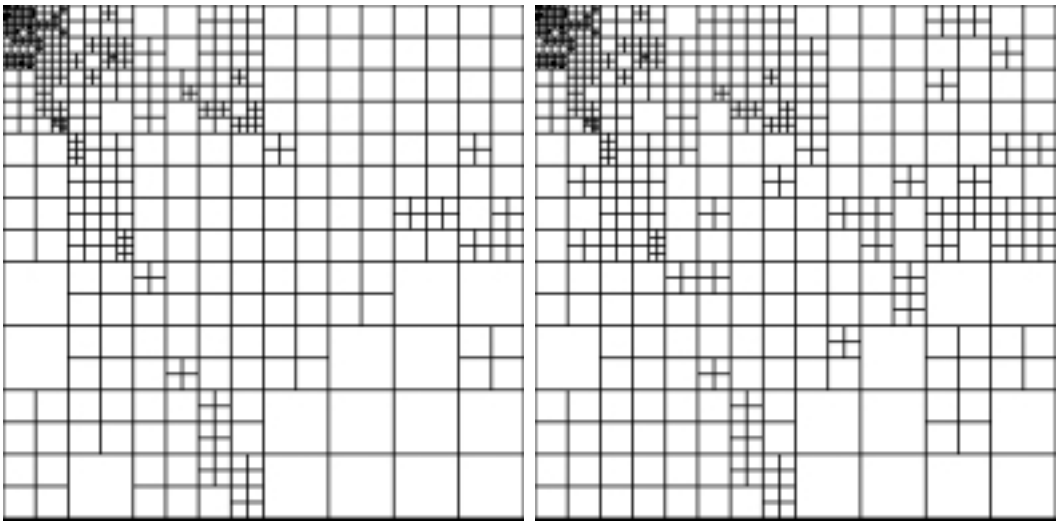


FIG. 7.12 – Meilleures bases originales et tatouées.

7.2.2 Détection de la marque

Détection avant attaque

Nous allons regarder le comportement à la détection de notre tatouage. L'image est stockée par compression JPEG de 100% de qualité (ce qui ne constitue pas une attaque). La figure 7.13 présente la réponse du détecteur à 1000 watermarques générées aléatoirement. La watermarque implantée dans l'image apparaît en position 500, elle est parfaitement détectée, la distance de Hamming est nulle.

Détection après attaque

L'attaque que nous faisons subir à l'image est une compression JPEG de 50% de qualité. La figure 7.14 présente les meilleures bases obtenues avant et après cette attaque. Quelques noeuds basses fréquences ont disparus, la détection ne sera pas bonne. En effet, la figure 7.15 montre les réponses du détecteur à 1000 watermarques, la marque implantée (en position 500) n'est pas détectée. La redondance de 2 (la même marque est inscrite deux fois dans l'image) ne suffit pas à rectifier les erreurs d'extraction.

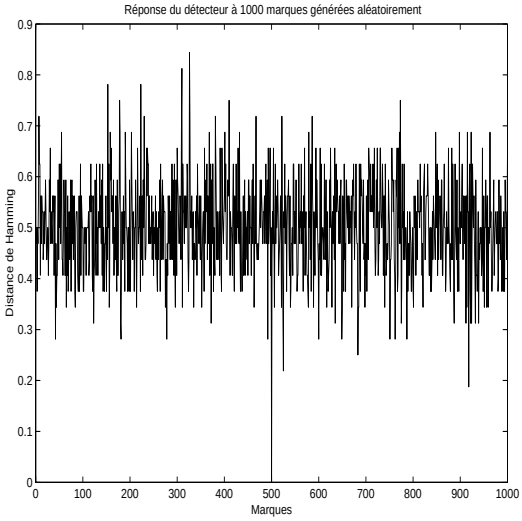


FIG. 7.13 – Réponse du détecteur à 1000 watermarques générées aléatoirement, notre marque apparaît en position 500

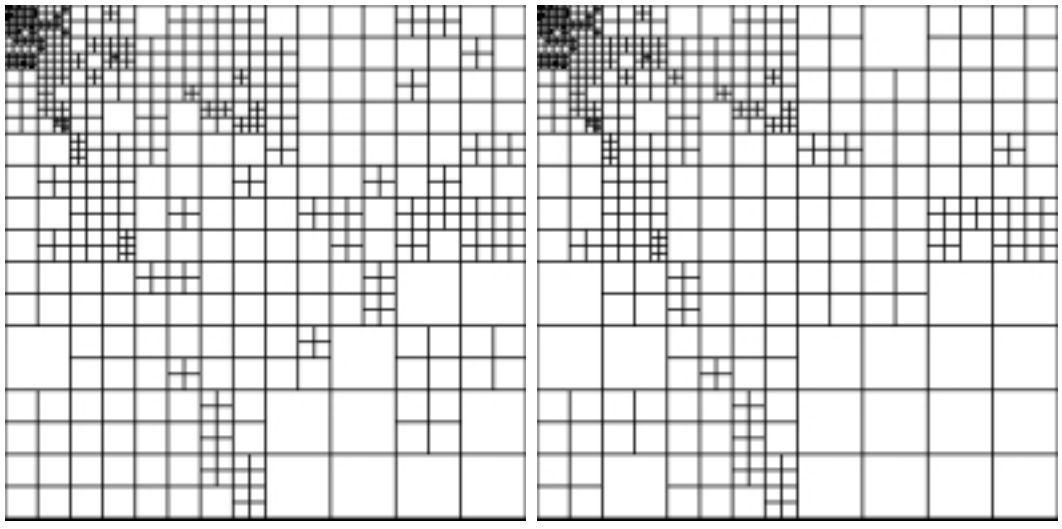


FIG. 7.14 – Meilleures bases avant et après une compression JPEG de 50% de qualité.

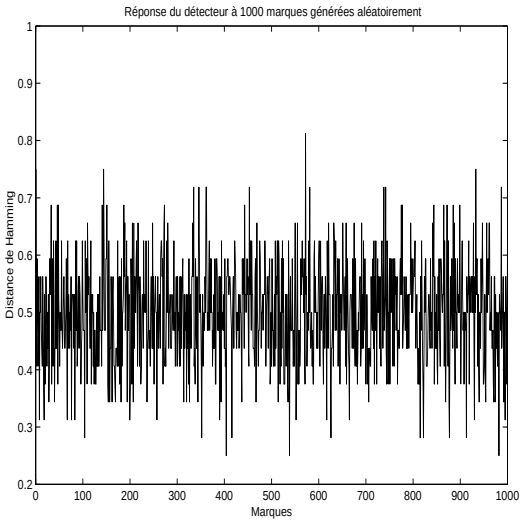


FIG. 7.15 – Réponse du détecteur à 1000 watermarques générées aléatoirement après une compression JPEG de coefficient de qualité 50%, notre marque apparaît en position 500

Conclusion

Ce premier essai est encourageant en ce qui concerne l'invisibilité du tatouage mais la détection donne de mauvais résultats après une attaque $JPEG$ de 50% de qualité. Pour améliorer la qualité, nous avons deux choix : augmenter la longueur de la marque (afin de rajouter de la redondance), c'est ce que nous proposons dans l'exemple 2 ou augmenter la force du tatouage ce qui constituera l'essai 3. Le tableau 7.1 présente les valeurs que nous utilisons pour les deux exemples qui suivront. La longueur m de la marque est exprimée en fonction de la longueur du message transmis (32 bits) et du coefficient de redondance.

TAB. 7.1 – Paramètres d'entrées choisis pour les exemples

Exemple	m	s	ε
Exemple1	32×2	$10^{-4.8}$	$s/10$
Exemple2	32×10	10^{-6}	$s/10$
Exemple3	32×2	$10^{-4.8}$	$3s$

7.3 Deuxième exemple : Augmentation de la longueur de la marque

7.3.1 Implémentation de la marque

La marque que nous choisissons est de longueur 320. Elle est composée d'un code de 32 bits répétés 10 fois. Le seuil de sélection de la meilleure base est choisi plus petit afin

de permettre la présence de plus de paquets dans la base. L'image tatouée ne présente pas de différence perceptible avec l'originale. Elle est présentée sur la figure 7.16. Le PSNR entre ces deux images est de 47.58 dB, ce qui est un bon résultat.

FIG. 7.16 – Image originale et image marquée

Les meilleures bases originales et modifiées sont présentées à la figure 7.17. Le choix d'un plus petit seuil entraîne l'augmentation du nombre des paquets.

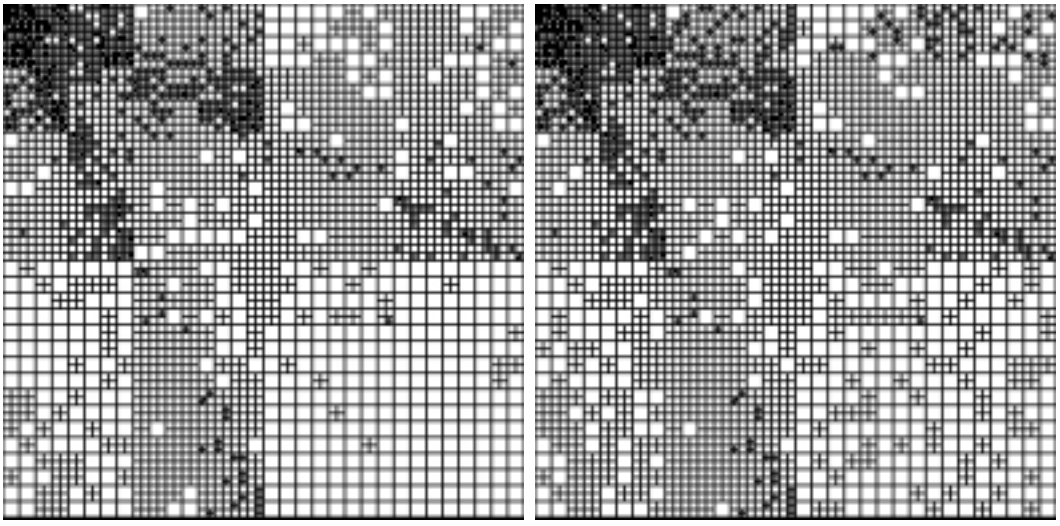


FIG. 7.17 – Meilleures bases originales et tatouées.

7.3.2 Détection de la marque

La détection de la marque donne les mêmes résultats que précédemment. Elle est parfaite avant attaque (figure 7.18(a)) et impossible après une compression JPEG de 50% de qualité (figure 7.18(b)).

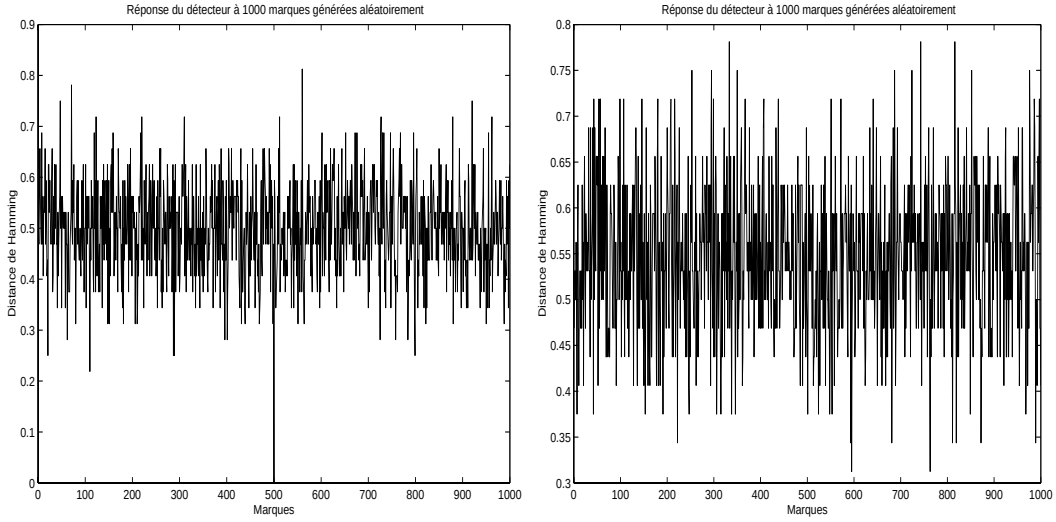


FIG. 7.18 – Réponses du détecteur avant et après compression JPEG de 50%.

On ne peut pas tirer de loi du comportement de la méthode de tatouage avec un seul résultat, il semble cependant que la redondance seule ne soit pas une solution efficace pour améliorer la robustesse.

7.4 Troisième exemple : Augmentation de la force du tatouage

La force du tatouage est augmentée significativement : $\varepsilon = 3s$. Cela signifie que l'énergie des paquets modifiés (les paquets fils des paquets exclus de la base) est augmentée à $4s$ au lieu de s. Les autres paramètres de la méthode ne changent pas.

7.4.1 Implémentation de la marque

La figure 7.19 montre les résultats que l'on obtient après tatouage. L'image tatouée présente des distorsions visibles, le PSNR est bas : 28.3dB. Des détails de ces deux images sont donnés à la figure 7.20. L'image différence est présentée à la figure 7.21 avec le même coefficient d'amplification qu'au premier exemple. Ici les modifications sont trop fortes, elles sont visibles.

FIG. 7.19 – Image originale et image marquée

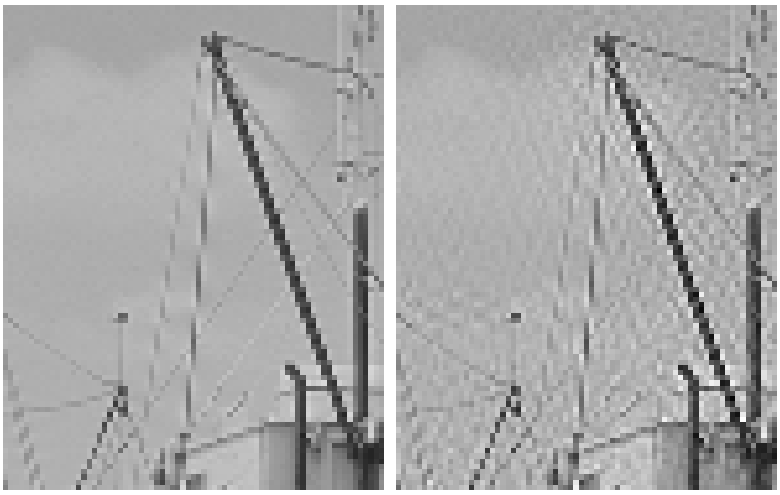


FIG. 7.20 – Image originale et image marquée, détails

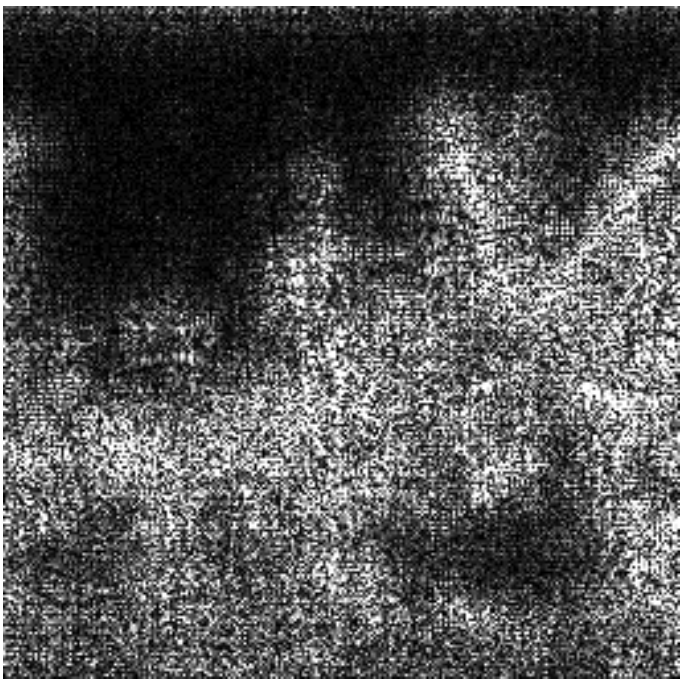


FIG. 7.21 – Image différence des images originale et marquée

7.4.2 Détection

La figure 7.22 montre le comportement du détecteur avant et après l'attaque compression JPEG de 50% de qualité. La détection est excellente et la marque est reconnue dans les deux cas. L'augmentation de la force du tatouage semble donner de bons résul-

tats en terme de robustesse. Cependant ce choix donne de mauvais résultats en terme d'invisibilité du marquage. On retrouve ici le compromis robustesse/invisibilité.

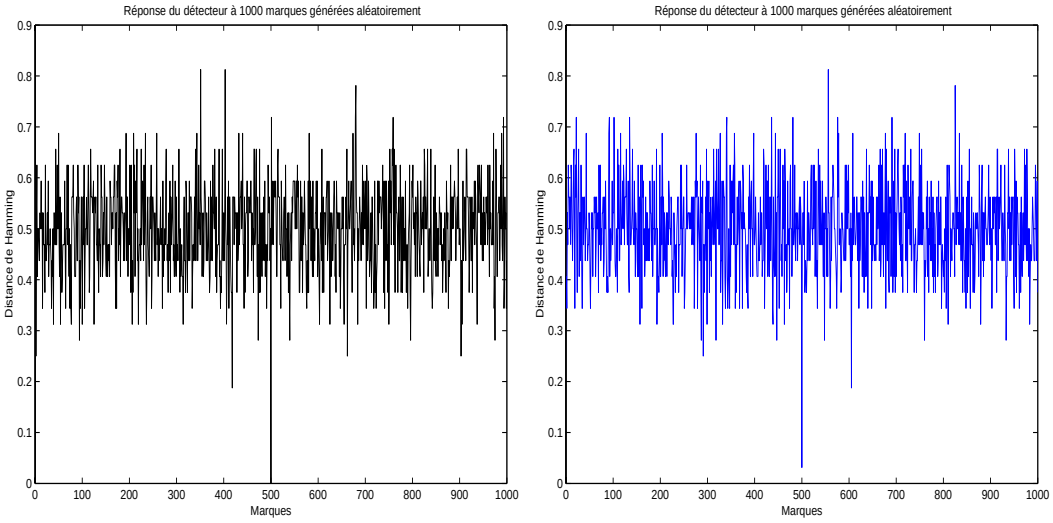


FIG. 7.22 – Réponses du détecteur avant et après compression JPEG de 50%.

7.5 Quatrième exemple : Tatouage de l'image fruit

Cet exemple consiste à tatouer une image présentant des zones uniformes plus nombreuses. Le tatouage est réalisé pour une valeur moyenne du coefficient de redondance $m = 7 \times 32$ bits. La force du tatouage est assez élevée $\varepsilon = 1.75s$, le seuil s est pris à $s = 10^{-5.2}$ afin d'obtenir suffisamment de paquets d'ondelettes.

7.5.1 Implémentation de la marque

La figure 7.23 montre les résultats que l'on obtient après tatouage. La version numérique de l'image tatouée présente des distorsions visibles, en particulier sur la poire. La version imprimée est de la même qualité que l'image originale. Le PSNR est très moyen : 31.89 dB.

FIG. 7.23 – Image fruit originale et image marquée

7.5.2 Détection

La figure 7.24 présente les différentes meilleures bases obtenues pour l'image originale et les images tatouées avant et après une compression JPEG de facteur de qualité de 50%. On remarque que la compression a modifié la structure de la base. Certains noeuds

présents dans la base tatouées ont disparus. Ces noeuds se situent principalement (mais pas uniquement) dans les basses fréquences de la décomposition. Il est important de noter que l'attaque change complètement la structure de la base : des noeuds présents à la fois dans la base originale et dans la base tatouée ont disparu. Pour cette image et ce choix du seuil, c'est la structure de la base originale qui est sensible à l'attaque et pas seulement celle modifiée par tatouage.

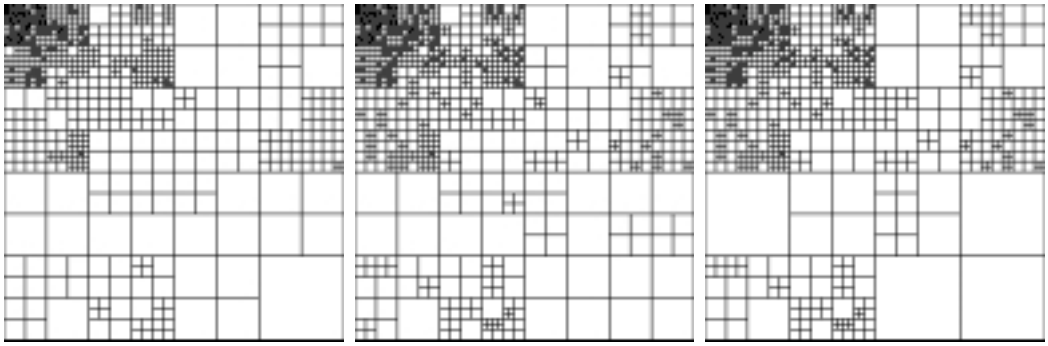


FIG. 7.24 – Meilleures bases originale et tatouées avant et après l'attaque par compression JPEG de 50% de qualité.

La figure 7.25 montre le comportement du détecteur après l'attaque compression JPEG de 50% de qualité. La détection est excellente et la marque est reconnue sans aucune erreur. Ce bon résultat est obtenu d'une part grâce au choix d'une force de tatouage élevée et d'autre part grâce à un coefficient de redondance assez grand qui permet ici de corriger les erreurs dues à l'attaque et que l'on a observées à la figure 7.12 et en particulier la non stabilité de la meilleure base.

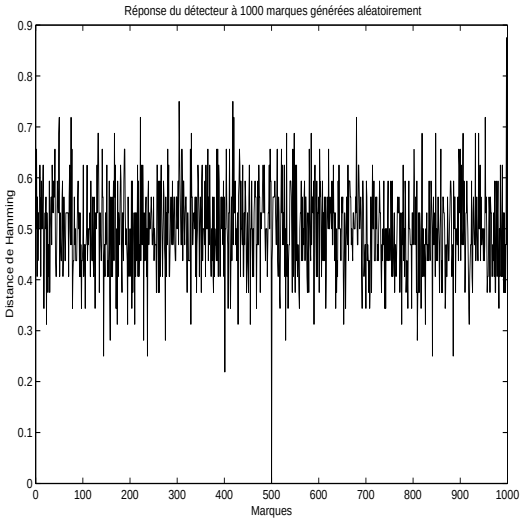


FIG. 7.25 – Réponses du détecteur après compression JPEG de 50%.

7.6 Conclusion

Bien que nous ne puissions pas conclure à partir des quelques exemples présentés ici, l'algorithme de tatouage semble prometteur. En effet, selon les valeurs de la force du marquage et celles du coefficient de redondance, le tatouage est soit invisible soit très robuste à la compression JPEG. Notre méthode présente de plus un atout important pour le tatouage des images : la marque peut être de longueur très variée. La suite de notre travail consistera à étudier les influences des différents paramètres (m, s et ε) sur les performances de la méthode et à les optimiser lorsque c'est possible.

Quatrième partie

Améliorations de la méthode de tatouage d'images par paquets d'ondelettes

Chapitre 8

Étude du comportement de la structure de la meilleure base face à diverses attaques

La sélection d'une meilleure base de paquets d'ondelettes constitue le coeur de notre méthode. Nous avons vu en effet que les composantes modifiées sont les paquets sélectionnés et que la marque est exprimée par des modifications de la structure de la base. Il est donc primordial que cette structure soit stable après une attaque de l'image. C'est à dire qu'elle doit rester identique si l'on fait subir à l'image une attaque qui ne la dégrade pas trop. Cette contrainte a été considérée lors du choix du critère de sélection de la meilleure base (voir le paragraphe 5.3). On ne sélectionne dans la meilleure base que des paquets possédant une énergie significative. Cependant, nous avons vu à travers les exemples donnés dans le chapitre 7 que la structure de la base n'était pas invariante si l'on attaquait l'image par une forte compression JPEG.

L'objectif de ce chapitre[1] est d'analyser la non invariance de la structure de la meilleure base aux attaques. Nous choisissons de faire cette analyse de façon expérimentale. Pour un ensemble d'images test composé de 8 images, nous calculerons trois meilleures bases pour des seuils de sélection s différents et nous étudierons leurs comportements face à un ensemble composé de 87 attaques. La première partie de ce chapitre présente la procédure de tests. Nous étudierons ensuite les résultats obtenus selon plusieurs paramètres. Le premier paramètre pris en compte sera évidemment le seuil s de sélection de la meilleure base. Puis nous regarderons les noeuds instables (ceux dont l'apparition ou la disparition modifient la structure de la base). Nous étudierons en particulier l'énergie de ces noeuds, ainsi que leur niveau de résolution et la bande de fréquence qu'ils occupent dans la meilleure base.

[1] Les résultats présentés dans ce chapitre et dans le chapitre 10 ont servi de base à la rédaction de l'article [57].

8.1 Définition et condition de stabilité de la base

Définition 4 *Une meilleure base B est dite stable pour une attaque donnée, si après attaque, la meilleure base B', calculée selon le critère énergétique, est telle que $B' = B$.*

Une condition nécessaire et suffisante La base B sera stable après attaque si et seulement si les noeuds sélectionnés par la base B sont sélectionnés par B'. On dira alors que ces noeuds sont stables ou robustes. En d'autres termes, si le noeud N_p est dans B et s'il n'est pas dans B', N_p est fragile ou instable.

8.2 Présentation des test numériques

Procédure de test Nous avons attaqué un ensemble de 8 images par un ensemble de 87 attaques. Pour chaque image, nous avons sélectionné trois bases issues de seuils de sélection différents ($s_1 = 10^{-5}$, $s_2 = 10^{-6}$ et $s_3 = 10^{-7}$). Nous avons étudié les modifications de ces bases après chaque attaque.

Ensemble test Cet ensemble est représenté à la figure 8.1, il est composé d'images de type cinéma, classiques en traitements d'images. Il contient les images appelées respectivement : «Barbara», «Lenna», «Bateau», «Caméra», «Pont», «Poivrons», «Singe» et «Oiseau». Toutes les images testées sont de dimension 256×256 et codées sur 8 bits par pixels.

FIG. 8.1 – Ensemble des images tests

Les attaques Comme il s'avère impossible de considérer toutes les attaques possibles, nous avons décidé de restreindre notre domaine d'étude à l'ensemble des 87 attaques présentes dans le logiciel Stirmark [5]. Je donne ci dessous une brève descriptions de ces attaques, plus d'informations sont disponibles dans [5].

- Les 8 premières attaques sont des "cropping" allant de 1% à 50% de la taille de l'image (figure 8.2).

- Dans les 5 suivantes, des colonnes et des lignes sont enlevées et d'autres dupliquées (figure 8.3). Ce type d'attaques est dangereux pour les schémas additif à étalement de spectre.
- Les 6 attaques suivantes concernent la taille de l'image (figure 8.4). L'image est uniformément rétrécie ou agrandie.
- Dans les attaques numéro 20 à 27 les proportions entre les dimensions horizontales et verticales sont modifiées (figure 8.5).
- Les trois attaques suivantes sont des rotations de petits angles.
- L'attaque 31 est le FMLR (figure 8.6)
- Les treize suivantes sont des rotations d'angles de plus en plus importants. Afin d'empêcher un prétraitement à la détection consistant à redresser l'image en détectant ses bords, l'image est croppée. Il n'apparaît que les parties significatives de l'image (figure 8.7).
- De 45 à 60, les attaques sont des combinées de rotations et de changements de taille. Contrairement aux cas précédents, l'image retrouve sa taille originale (figure 8.8).
- Les 6 attaques suivantes sont des étirements (figure 8.9).
- Les 3 suivantes sont des filtrages linéaires
- L'attaque 70 est l'attaque stirmark. Elle consiste à faire de petites déformations géométriques invisibles sur l'image (figure 8.10).
- L'attaque 71 est un filtrage Gaussien (figure 8.11)
- L'attaque 72 est un filtrage passe haut (figure 8.12).
- Les trois suivants sont filtrages moyenneurs (figure 8.13)
- Les dernières attaques sont des compressions JPEG allant de 90% à 10% de qualité (figure 8.14).

FIG. 8.2 – Image attaquée par un cropping de 25%

FIG. 8.3 – Image avec 17 lignes et 5 colonnes enlevées

FIG. 8.4 – Image de taille réduite de moitié

FIG. 8.5 – Image étirée de 110% en horizontal

FIG. 8.6 – FMLR

FIG. 8.7 – Rotation de 45 puis cropping

FIG. 8.8 – Rotation de 45, l'image est redimensionnée

FIG. 8.9 – Étirements

FIG. 8.10 – Attaque stirmark

FIG. 8.11 – Filtrage gaussien

FIG. 8.12 – Filtrage passe haut

FIG. 8.13 – Filtrage moyenneur

FIG. 8.14 – Compression JPEG avec 10% de qualité

Prétraitements aux calculs des bases modifiées L'algorithme de décomposition d'une image en meilleure base requiert une image de dimension $N \times N$, N étant une puissance de 2. Lorsque la taille de l'image est modifiée par transformation, nous avons décidé de restaurer la taille initiale de l'image sans a priori sur l'attaque.

- si l'image a été agrandie, on en coupe les bords.
- si la taille de l'image est plus petite que celle de l'image originale, on procède par miroir, l'image attaquée est centrée et les bordures sont les symétries de l'image.

Qualités des attaques Les attaques présentées ci-dessus dégradent plus ou moins l'image. La figure 8.15 présente l'évolution de la valeur du PSNR de chaque image test en fonction de l'attaque proposée. Les abscisses représentent les différentes attaques selon l'ordre que nous avons donné ci-dessus. La valeur du PSNR de la plupart des images est très bas (inférieur à 30 dB). Ceci indique que certaines images attaquées peuvent ne pas être de bonne qualité. Rappelons cependant qu'il est dangereux de se contenter de la mesure du PSNR pour juger de la qualité des images. Les premières attaques, par exemple, sont des «cropping» de l'image, elles sont forcément de bonne qualité. D'autres attaques comme les filtrages présentés aux figures 8.11, 8.12 et 8.13 dégradent fortement la qualité de l'image. Notre but est simplement de remarquer que certaines attaques rendent les images non exploitables commercialement, pour celles-ci, la robustesse du tatouage n'est pas cruciale.

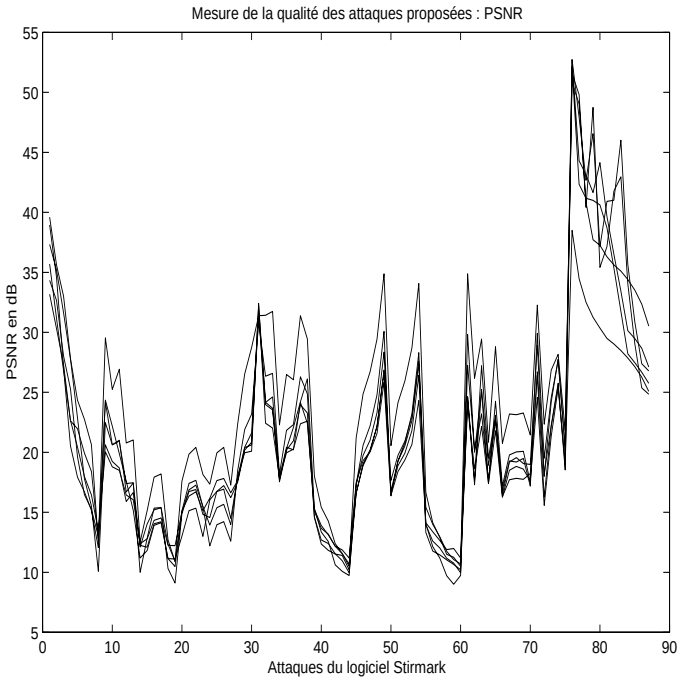


FIG. 8.15 – Valeurs du PSNR pour les images tests selon les attaques du logiciel Stirmark

8.3 Stabilité et choix du seuil de sélection de la meilleure base

Nous avons calculé pour trois seuils s, le nombre de noeuds stables après chaque attaque. Nous nous intéressons uniquement aux noeuds présents dans la structure de B et absents de la structure de B'. En effet, nous avons choisi de modifier ces noeuds : la clef K pointe uniquement des noeuds de B. Si la clef sélectionnait des noeuds quelconques de l'arbre, nous aurions dû prendre en compte les «apparitions» de noeuds, c'est à dire les noeuds absents de B et présents dans B'. De plus, nous ne nous intéresserons pas aux noeuds de B appartenant au dernier niveau de décomposition (niveau 8). En effet, l'instabilité de ces noeuds n'aura pas de conséquence sur notre méthode : ces noeuds ne pouvant pas être modifiés, ils ne sont jamais pointés par K.

La figure 8.16 représente les résultats de ce test pour l'image Barbara. L'axe des ordonnées donne le nombre de noeuds robustes de la base B après une modification, l'axe des abscisses donne le numéro de l'attaque. La courbe dessinée avec des "+" représente les résultats obtenus pour un seuil de $10^{-7}E_0$, celle avec les "△", un seuil de $10^{-6}E_0$, la dernière, un seuil de $10^{-5}E_0$, E_0 étant l'énergie totale de l'image attaquée.

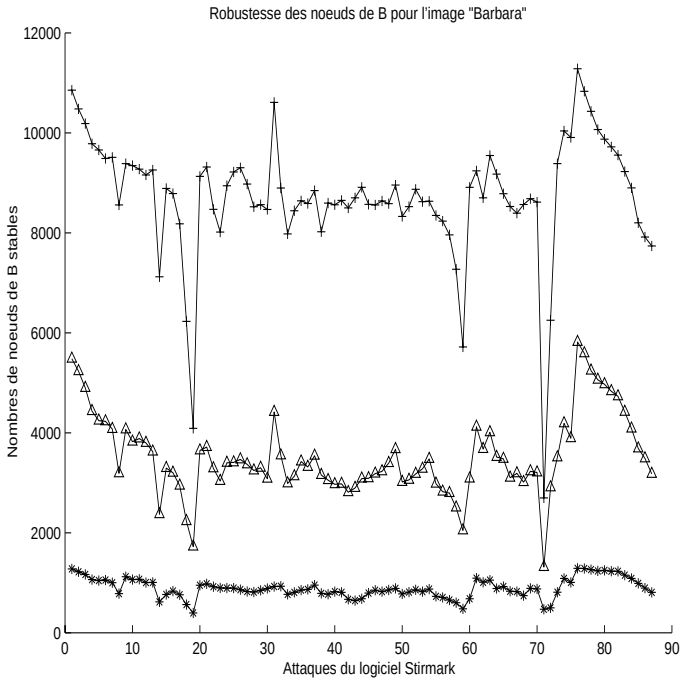


FIG. 8.16 – Nombre de noeuds de B stables pour les attaques du logiciel Stirmark et pour trois seuils, pour l'image Barbara.

Les courbes figure 8.3 sont les résultats obtenus pour les 7 images suivantes.

Les attaques les plus dangereuses Nous remarquons que même si le comportement de la robustesse des noeuds varie en fonctions des attaques, quelque soit le seuil, les

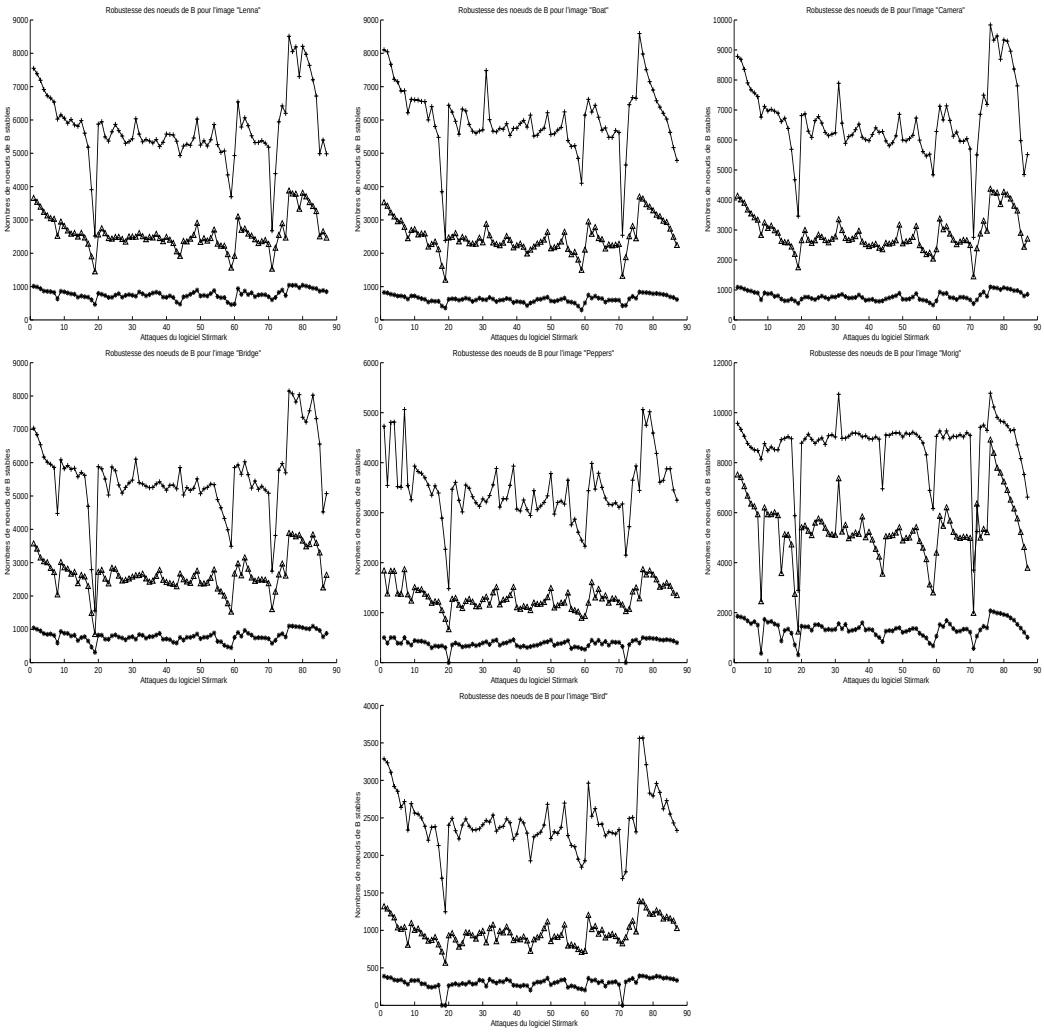


FIG. 8.17 – Nombres de noeuds de B stables pour les attaques du logiciel Stirmark et pour trois seuils, pour les images test.

courbes ont la même allure. En particulier, les attaques 19, 59 et 71 donnent toujours de très mauvais résultats. L'attaque 19 correspond à une augmentation de la taille de l'image de 200%. La 59 est une rotation de 45 degré suivit d'un redimensionnement (voir figure 8.8) et l'attaque 71 est un filtrage gaussien (voir figure 8.11).

Pour la première attaque, les mauvais résultats s'expliquent par le prétraitement qui ne convient pas à ce type d'attaque. En effet, il n'y a aucune raison pour que la meilleure base du quart de l'image ressemble à la meilleure base de cette image. Pour la deuxième attaque, ce n'est pas la rotation qui donne de mauvais résultats, en effet, les rotations seules ne sont pas des attaques aussi dangereuses (ce sont les attaques de numéro 32 à 45). C'est donc le redimensionnement de l'image qui donne de mauvais résultats, pour les même raisons que pour l'attaque 19.

L'attaque par filtrage Gaussien constitue une attaque dangereuse pour notre méthode : en filtrant les fréquences, la composition fréquentielle de l'image est changée, l'arbre de décomposition est bouleversé. La meilleure base est donc fragile à cette attaque. Cependant, la figure 8.11 montre que cette attaque dégrade beaucoup la qualité de l'image. De plus, le PSNR est inférieur à 30. Cette attaque est donc très dégradante, de ce point de vue, elle ne constitue pas un réel problème.

Autres attaques La stabilité des bases est assez bonne pour des compressions JPEG de grand coefficients de qualité ainsi que pour des petits cropping.

Pour l'image Poivrons (en cinquième position sur la figure 8.3) l'effet cumulé du cropping et du prétraitement conduit à effets de bords impressionnants.

Influence du choix du seuil Nous observons que plus le seuil de sélection de la meilleure base est choisi petit, plus la courbe de robustesse est accidentée. Pour une grande valeur du seuil, la robustesse semble meilleure. Le nombre de noeuds présents dans les meilleures bases est très différent selon la valeur du seuil considéré, c'est pourquoi, il peut sembler préférable de considérer le *pourcentage* des noeuds stables.

La figure 8.18 représente le pourcentage de noeuds stables par meilleure base selon les attaques, pour l'image Barbara. La courbe tracée en traits pleins est obtenue pour $s = 10^{-5}$, en pointillés $s = 10^{-6}$ et en points $s = 10^{-7}$.

Les courbes du pourcentage de noeuds robuste obtenues pour les autres images sont représentées figure 8.3.

Pour l'image Barbara, les meilleurs résultats semblent être obtenus pour un seuil s soit grand, soit petit. Pour l'image Singe, le choix d'un petit seuil est le meilleur. Pour les autres images, on ne peut pas conclure à un résultat.

Conclusion Le choix du seuil de sélection s est crucial dans notre méthode, il détermine en effet la longueur du marquage et la structure de la base. En terme de robustesse, l'étude présentée ici ne permet pas de conclure sur le choix de la valeur du seuil. Cependant, le pourcentage des erreurs étant relativement constant selon le seuil choisi, cette étude nous incite à utiliser le cas où la base est composée du plus grand nombre de noeuds (cas où le seuil est petit). En effet, nous pourrons alors compenser le manque de

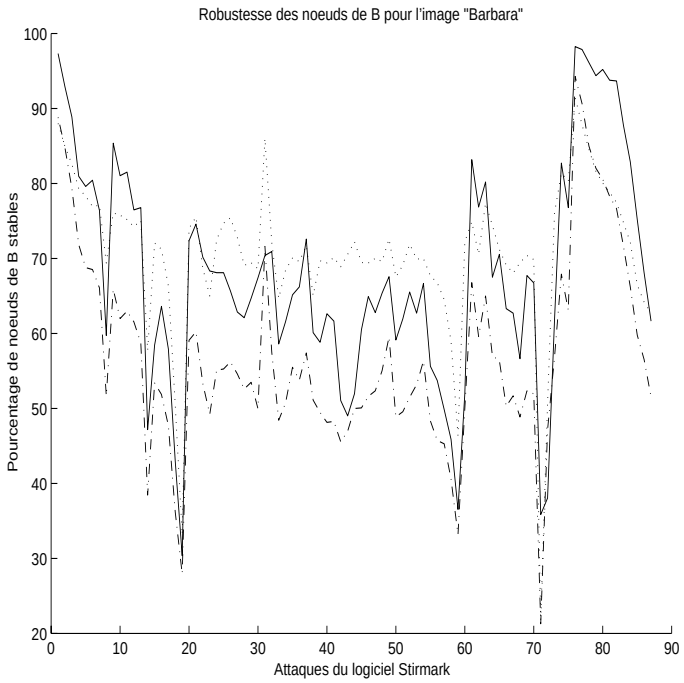


FIG. 8.18 – Pourcentage de noeuds de B stables pour les attaques du logiciel Stirmark et pour trois seuils, pour l'image Barbara.

stabilité de la base en utilisant un grand coefficient de redondance lorsque nous insérons la marque. C'est par exemple ce qui se produit dans l'exemple 8.3.

Dans le paragraphe 10, nous présenterons une étude plus poussée permettant d'optimiser un critère de stabilité de la meilleure base en fonction du seuil de sélection.

8.4 Étude de l'énergie des noeuds instables

La construction de la meilleure base se fait par seuillage : on compare les énergies des noeuds avec un seuil. Les noeuds d'énergie proche de ce seuil sont a priori plus sensibles aux attaques. Il suffit d'une petite diminution de leur énergie pour qu'ils disparaissent de la structure de la meilleure base. Ce sont alors leurs pères qui sont sélectionnés à leur place. Cette instabilité des noeuds de petite énergie à des conséquences très importantes pour la structure de la base. En effet, le père étant sélectionné, aucun noeud appartenant à l'arbre de racine le père ne pourra être sélectionné (on a une structure de base). Ceci signifie que cette forme d'instabilité provoque la destruction de la structure portée par l'arbre de racine le père de ce noeud. Si un noeud d'énergie trop faible disparaît de la structure de la base, ses trois frères disparaîtront. L'instabilité d'un noeud entraîne au minimum celle de 3 autres noeuds.

L'objectif de ce paragraphe est de présenter l'étude de l'instabilité des noeuds selon leur énergie. La figure 8.20 présente l'histogramme de l'énergie des paquets de la base B pour le seuil $s_1 = 10^{-5}$ (sans les noeuds appartenant au dernier niveau de la décom-

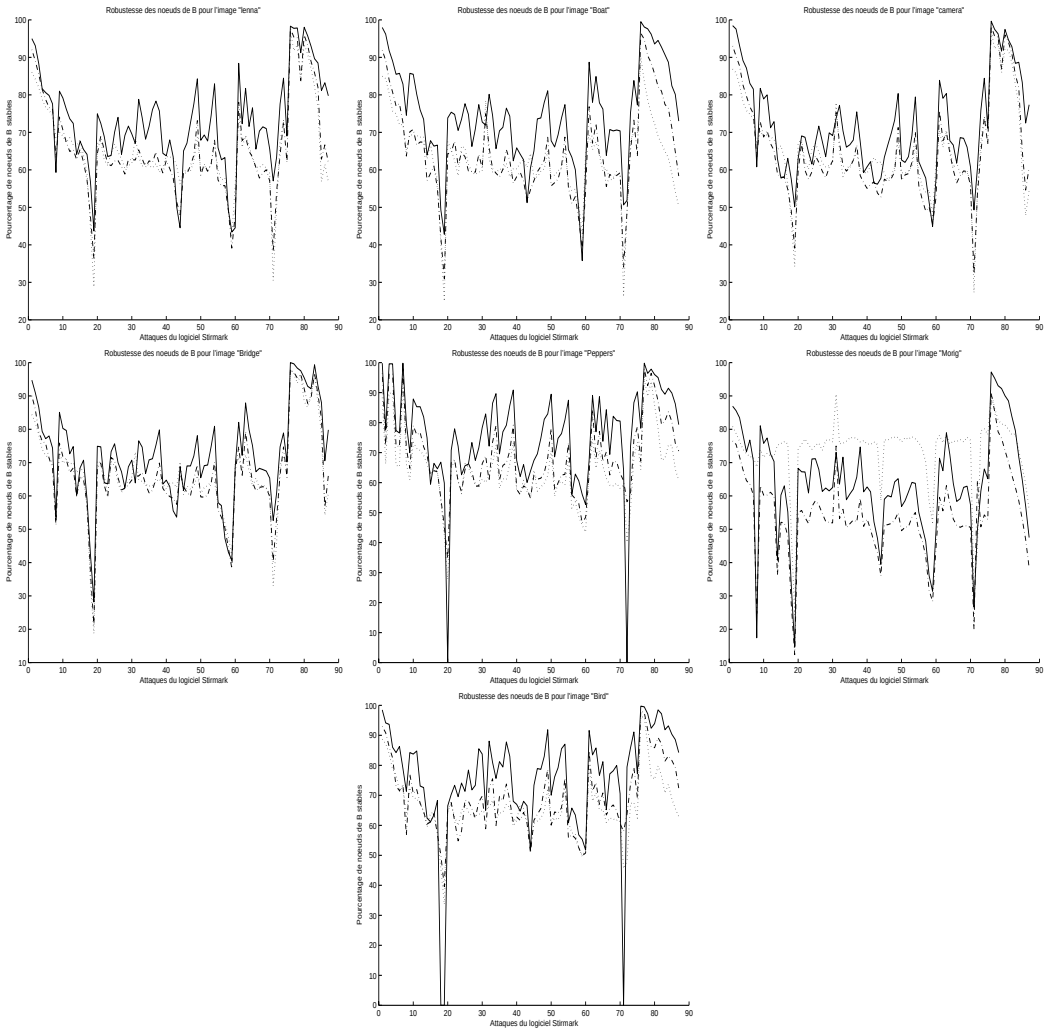


FIG. 8.19 – Pourcentage de noeuds de B stables pour les attaques du logiciel Stirmark et pour trois seuils, pour les images test.

position). Pour cette base, 70% des noeuds sont d'énergie comprise entre s_1 et $4s_1$. Ce résultat correspond bien à notre critère. La figure 8.21 présente le même histogramme pour un seuil de sélection $s_3 = 10^{-7}$, les valeurs des énergies sont plus étalées, le pic du diagramme est obtenu pour une valeur d'énergie de $4s_3$.

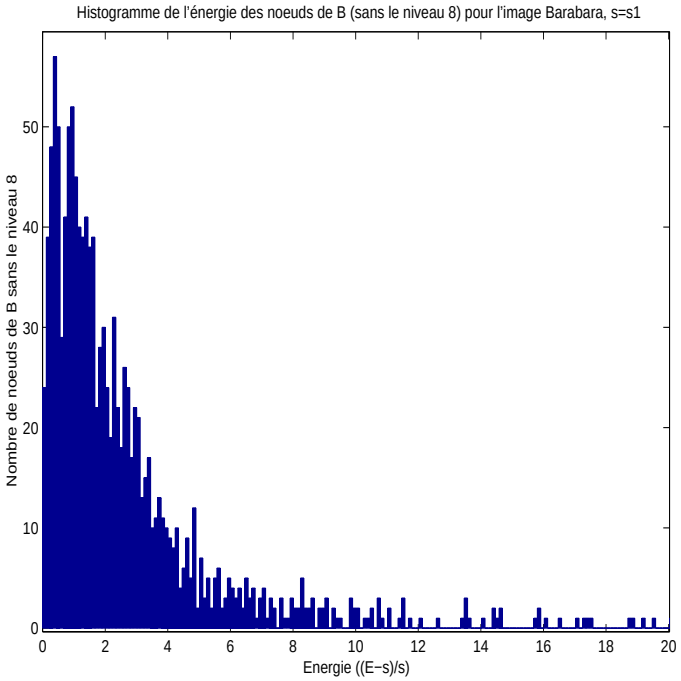


FIG. 8.20 – Histogramme de l'énergie des noeuds de la base pour Barbara, $s = 10^{-5}$

La figure 8.22 présente l'histogramme des énergies des paquets fragiles pour la base obtenue avec le seuil s_3 et pour toutes les attaques cumulées. Nous écartons les attaques 19, 59 et 71, qui ne nous semblent pas représentatives. L'histogramme a la même forme générale que celui présenté à la figure 8.21. Cela semble indiquer que les attaques touchent tous les vecteurs indifféremment de leur énergie. Cependant, le pic du diagramme est obtenu pour une valeur de l'énergie de $2,5s_3$. Ceci implique que les paquets de petite énergie sont moins robustes que les autres.

La figure 8.23 représente pour les 8 images, et pour chaque seuil, le pourcentage des noeuds fragiles qui ont une énergie initiale $E_i < 2s$. De même qu'auparavant, la courbe en trait plein représente les résultats obtenus pour $s_1 = 10^{-5}$, en pointillés $s_2 = 10^{-6}$ et en points $s_3 = 10^{-7}$. Pour les deux seuils s_1 et s_2, plus de 20% des noeuds fragiles sont des noeuds d'énergie inférieure à $2s$. pour le troisième choix du seuil, les résultats sont moins probants. Selon les images, le comportement change : l'image Singe qui est très texturée n'a pratiquement aucun noeud fragile proche du seuil s_3. Pour l'image Barbara, nous avons vu que le maximum de noeuds fragiles étaient d'énergie proche de $2.5s_3$.

Conclusions Comme nous l'avons rappelé au début de ce paragraphe, il est difficile d'analyser la robustesse des noeuds de la base. On ne peut pas savoir si un noeud est

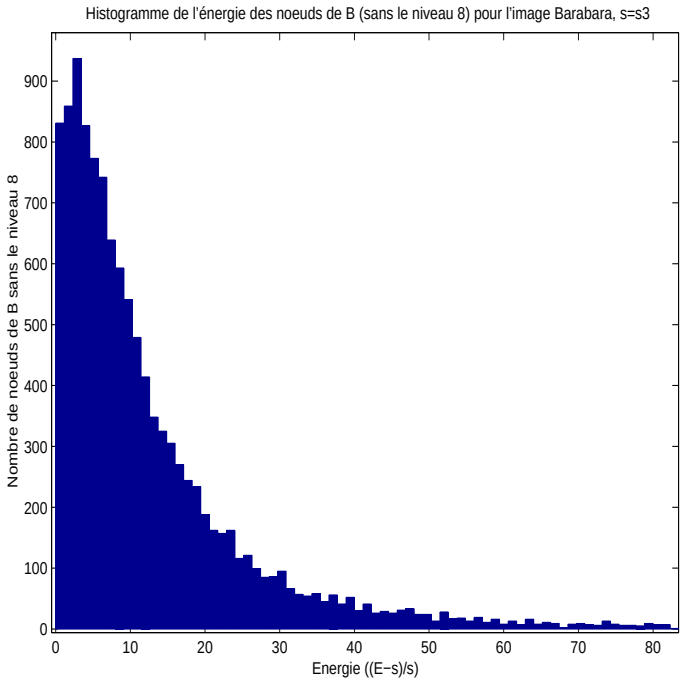


FIG. 8.21 – Histogramme de l'énergie des noeuds de la base pour Barbara, $s = 10^{-7}$

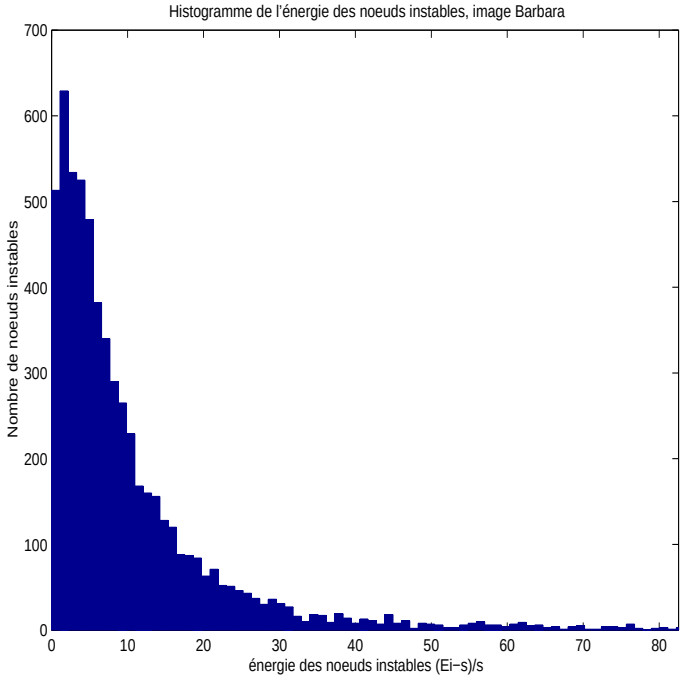


FIG. 8.22 – Histogramme de l'énergie des noeuds instables pour Barbara, seuil $s = 10^{-7}$

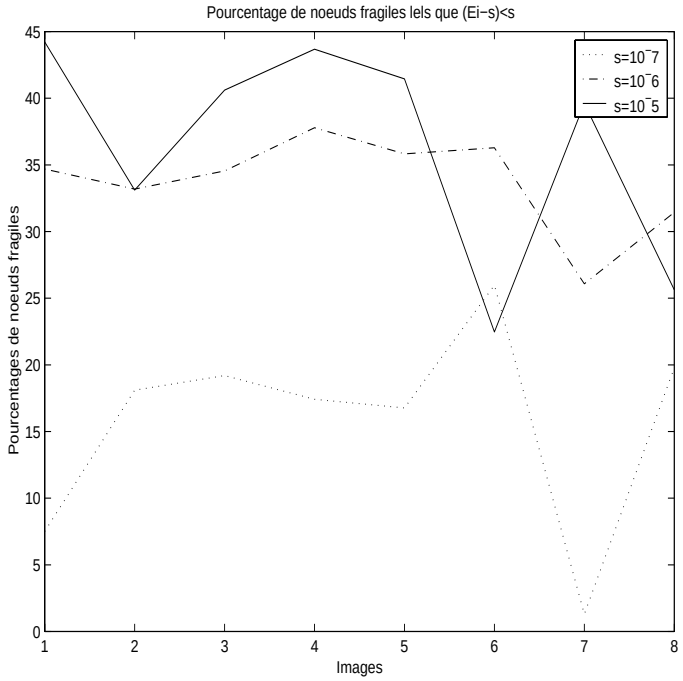


FIG. 8.23 – Pourcentage des noeuds fragiles dont l'énergie est inférieure à $2s$.

fragile parce que son énergie a changé ou si sa fragilité provient de la construction de la base et de l'instabilité d'un autre noeud.

Cependant, nous avons vu qu'une grande proportion des noeuds instables était de petite énergie. Cette étude nous encourage à utiliser une grande valeur de la force du tatouage ε. Nous avons vu lors des premiers exemples (voir le paragraphe 7) que la robustesse était alors améliorée.

De plus, nous proposerons au paragraphe 9 d'ajouter une étape dite de *stabilisation* à la méthode de tatouage. Cette étape consistera modifier les paquets de trop petite énergie ainsi que ceux de très grande énergie : les noeuds d'énergie trop proches du seuil en seront éloignés.

8.5 Étude selon l'échelle et la fréquence

Étude selon l'échelle Pour chacune des images étudiées et chaque modification on calcule le pourcentage de noeuds fragiles pour chaque niveau de l'arbre par rapport à sa contribution dans la meilleure base. Ces pourcentages sont tracés figures 8.24, et 8.25. La courbe en trait plein représente la contribution de l'avant dernier niveau de l'arbre (ici 7), les gros pointillés le niveau 6, les pointillés fin le niveau 5 et les étoiles le niveau 4. Sur chaque courbe, on précise le nombre de noeuds de chaque niveau dans la meilleure base initiale. Le test est réalisé pour un seuil de sélection de 10^{-7}.

Sur les graphiques 1 de la première figure et 3 de la seconde, on voit nettement que

le dernier niveau considéré est plus stable que l'avant dernier, ce qui paraît moins clair sur les autres graphiques. Les courbes correspondant au niveau 5 sont très accidentées, celles correspondant aux niveaux 4 sont encore plus mauvaises, elles atteignent souvent 100% d'instabilité.

Les fortes variations des courbes des premiers niveaux sont les conséquences du faible nombre de noeuds de ce niveau dans les bases. De même le nombre très important de noeuds dans le dernier niveau lisse les courbes de pourcentage. Les représentants de chaque niveau des bases ne permettent donc pas de conclusions significatives. Il reste cependant que les contributions des derniers niveaux sont les plus sûres pour une attaque quelconque.

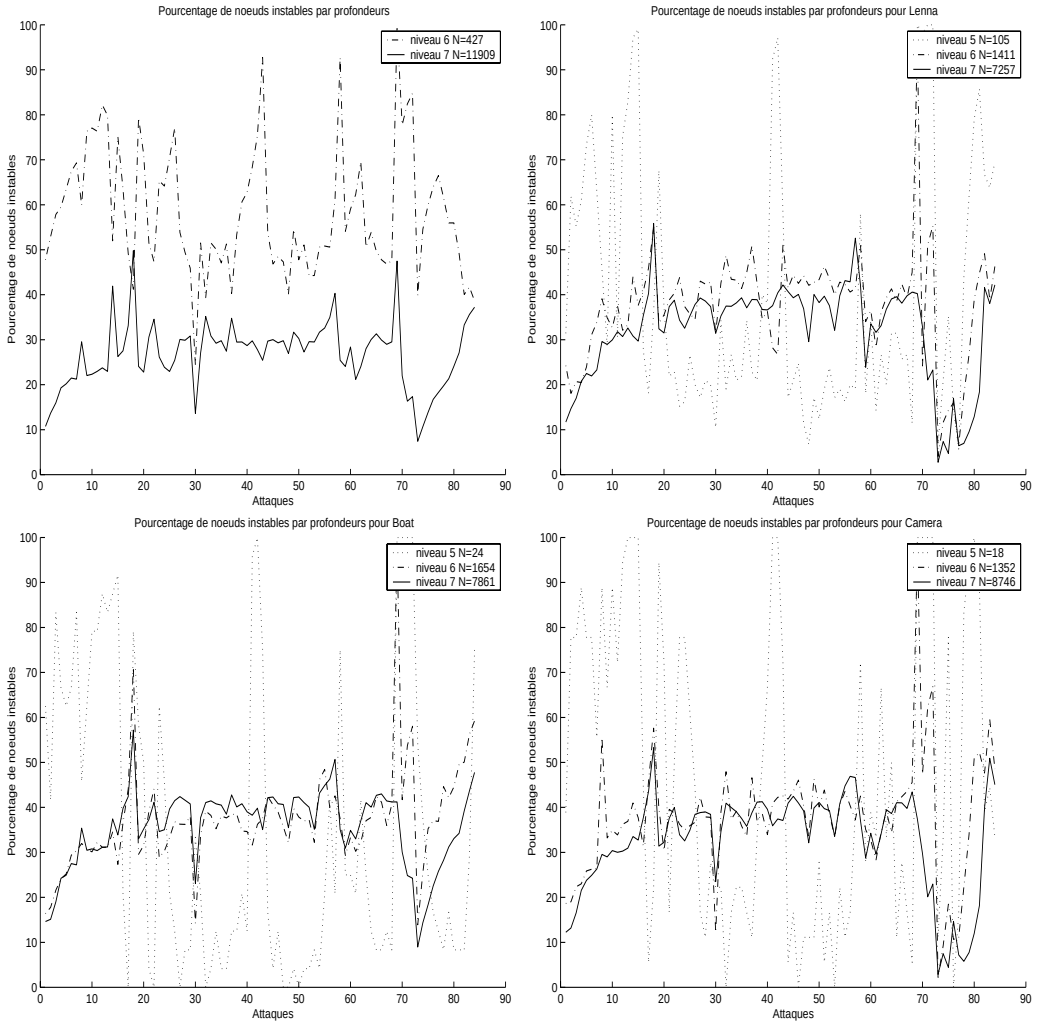


FIG. 8.24 – Pourcentages des noeuds de B instables pour les images Barbara, Lenna, Bateau et Caméra pour les attaques du logiciel Stirmark et pour un seuil de sélection de 10^{-7}

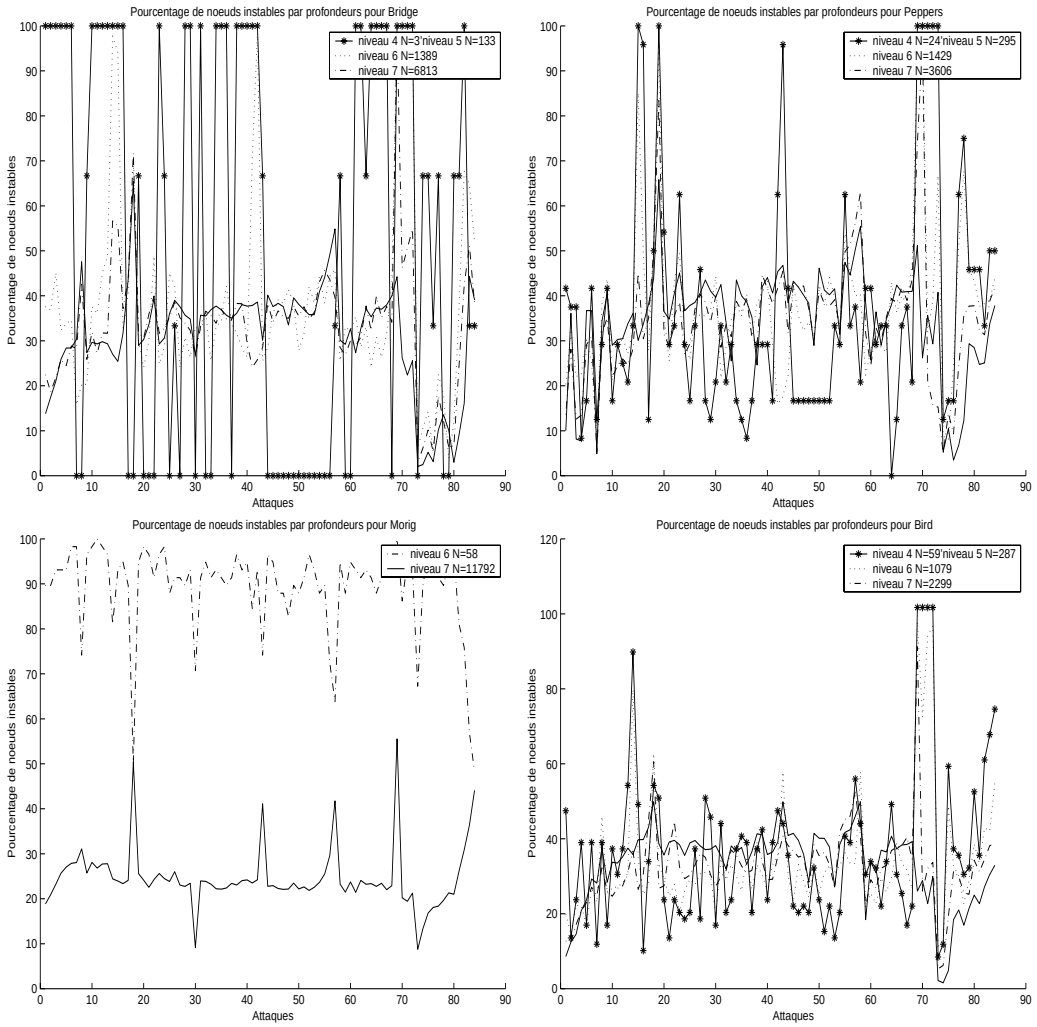


FIG. 8.25 – Pourcentages des noeuds de B instables pour les images Pont, Poivrons, Singe et Oiseau pour les attaques du logiciel Stirmark et pour un seuil de sélection de 10^{-7}

Conclusion Comme nous ne possédons aucun à priori sur les attaques que l'image est susceptible de subir, nous nous bornerons à considérer pour le codage les trois avant derniers niveaux de l'arbre en avantageant les sélections des noeuds sur l'avant dernier niveau. La profondeur totale de l'arbre de décomposition est p, nous implémenterons la marque sur les profondeurs $p-3$, $p-2$, $p-1$.

Étude selon les fréquences Nous présentons figures 8.26 à 8.29 les histogrammes cumulés des bandes de fréquences auxquelles appartiennent les noeuds instables. Les deux directions de fréquences sont présentées séparément et chacune est accompagnée de l'histogramme représentant la répartition des noeud dans la base initiale.

Prenons par exemple l'analyse des fréquences verticales de Barbara (première image de la figure 8.26). Le premier histogramme montre que toutes attaques cumulées, les noeuds hautes fréquences sont plus représentés parmi les noeuds instables que les noeuds basses fréquences. L'histogramme du dessous présente la répartition des noeuds de la base B. On voit que cette répartition est presque constante sur tout l'espace des fréquences. On peut donc conclure sur cet exemple que les hautes fréquences sont moins stables que les basses.

Si l'on observe l'image Oiseau (figure 8.29), cette tendance n'est plus vrai, les hautes fréquences ne sont pas plus représentées parmi les noeuds instables.

Conclusion On ne peut pas tirer d'enseignements de la répartition des noeuds selon leurs positions fréquentielles, on traitera donc les noeuds hautes ou basses fréquences de la même façon.

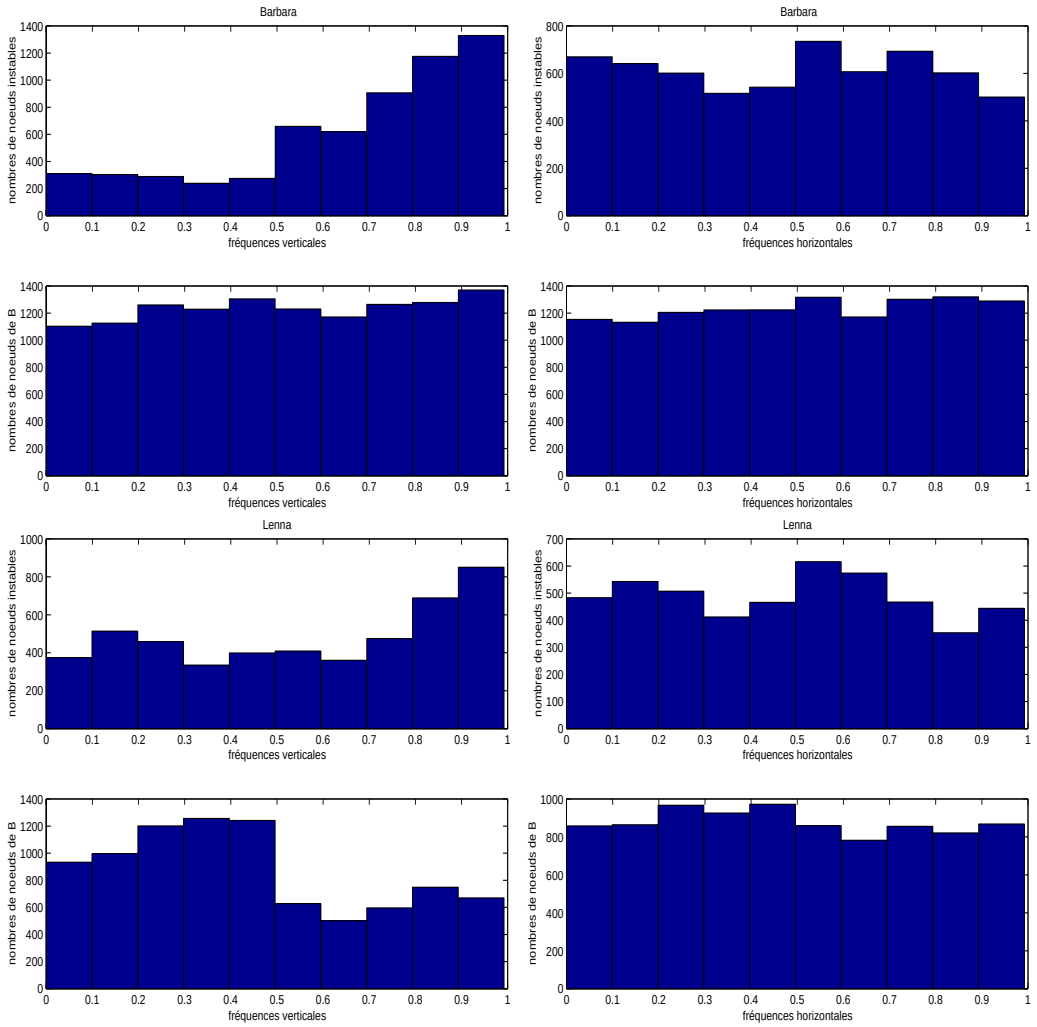


FIG. 8.26 – Histogrammes cumulés des bandes de fréquences auxquelles appartiennent les noeuds instables pour les images Barbara et Lenna

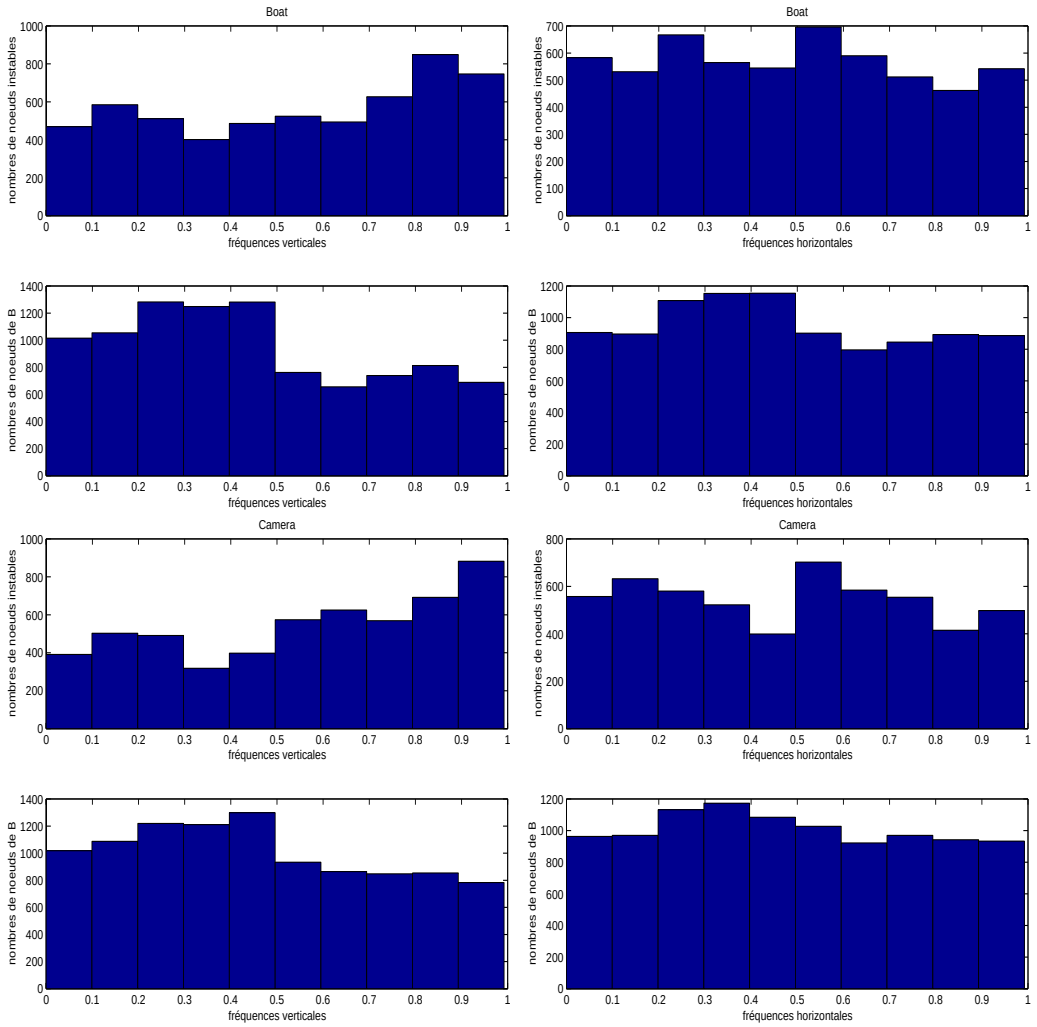


FIG. 8.27 – Histogrammes cumulés des bandes de fréquences auxquelles appartiennent les noeuds instables pour les images Bateau et Caméra

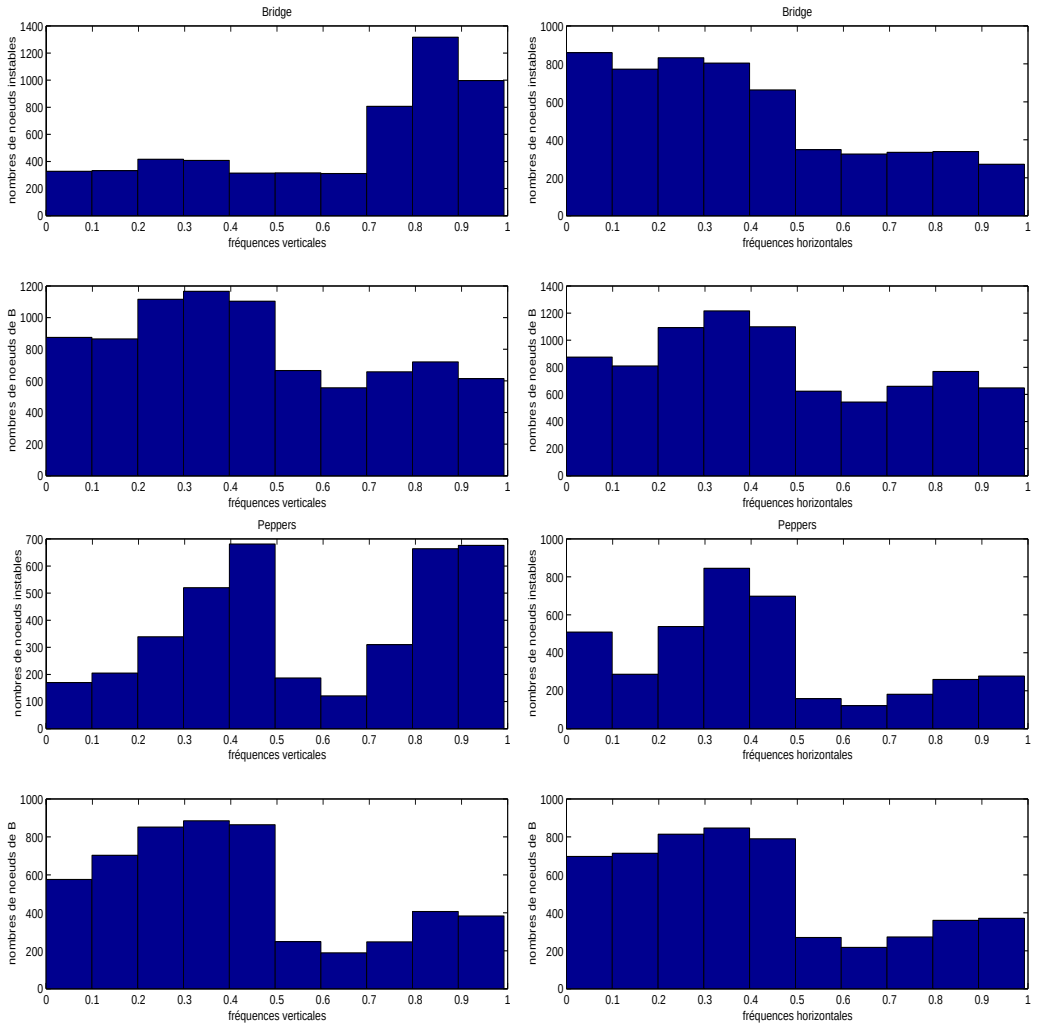


FIG. 8.28 – Histogrammes cumulés des bandes de fréquences auxquelles appartiennent les noeuds instables pour les images Pont et Poivron

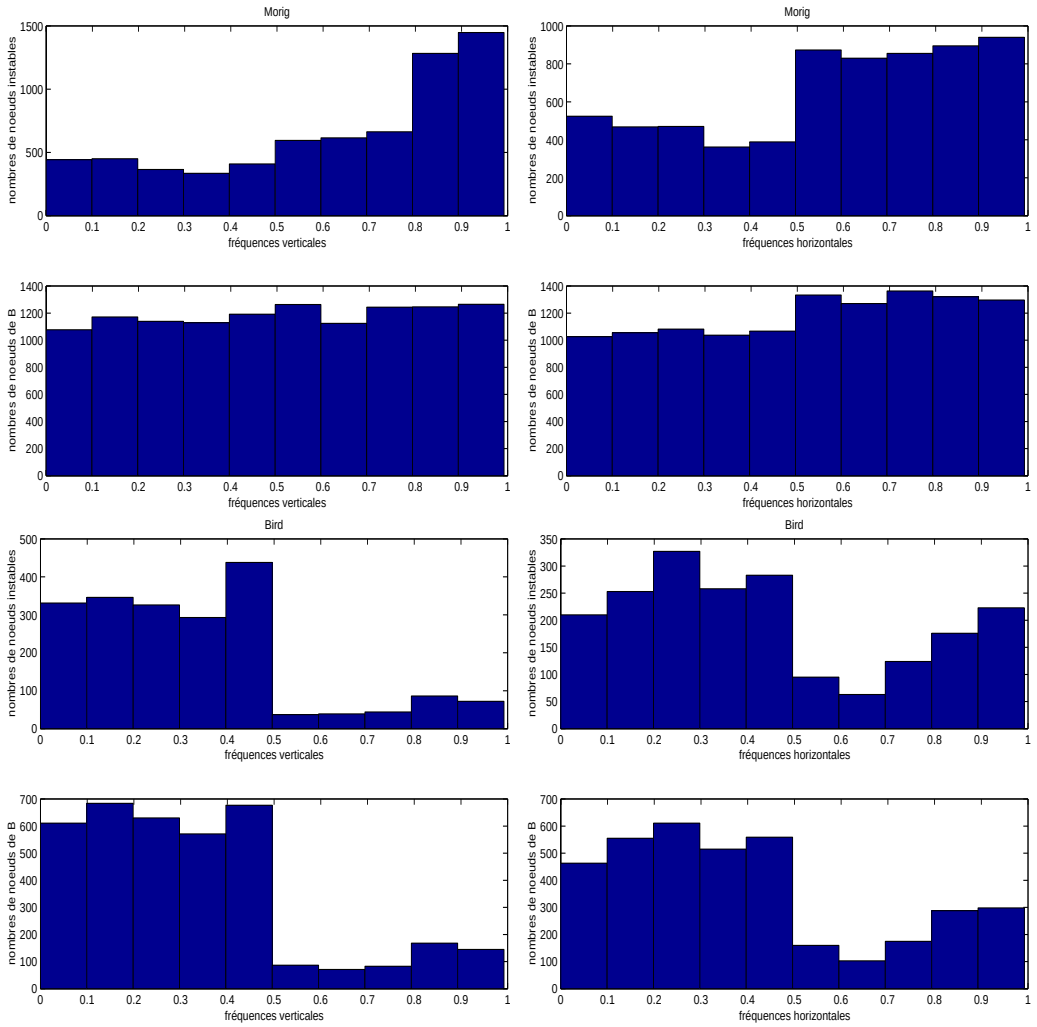


FIG. 8.29 – Histogrammes cumulés des bandes de fréquences auxquelles appartiennent les noeuds instables pour les images Singe et Oiseau

Chapitre 9

L'étape de stabilisation de la structure de la base

Le but de cette étape est de rendre la meilleure base plus stable. Nous avons vu paragraphe 8.4 qu'une forte proportion des noeuds instables ont une énergie proche du seuil, nous allons donc modifier cette énergie.

9.1 Description de l'étape de stabilisation

Soit un noeud N_i et ses 4 fils que l'on note $\{N_j^i\}_{j=[1..4]}$. Les énergies de ces noeuds seront notées E_i pour le noeud père et E_j^i pour les noeuds fils. Ces énergies seront modifiées, elles deviendront respectivement E_i^* et E_j^{i*}.

La décomposition en paquets d'ondelettes préserve l'énergie, on a donc la relation $E_i = \sum_{j=1}^{4} E_j^i$.

Noeuds potentiellement instables

Le noeud N_i est considéré potentiellement instable dans les deux cas suivants :
- 1 si son énergie est très petite : $s \leq E_i < s + \varepsilon_1$ avec ε_1 «petit».
- 2 si les énergies de ses fils sont très grandes : $\inf_j(E_j^i) > s - \varepsilon_2$ avec ε_2 «petit».

Dans le premier cas, si l'énergie du noeud est diminuée après une attaque, c'est son père qui sera sélectionné dans la meilleure base. Dans le second cas, si les énergies des fils augmentent suffisamment, ils seront sélectionnés dans la base.

La deuxième condition implique que E_i vérifie la relation suivante : $E_i > 4s - 4\varepsilon_2$.

Modifications de l'énergie de ces noeuds

- Dans le premier cas, on augmentera l'énergie du noeud selon :

$$E_i^* = s + \varepsilon_1 \tag{9.1}$$

– Dans le second cas, on diminuera l'énergie du fils possédant la plus petite énergie. Soit $j_0 \in 1,4$ tel que $\inf_j(E_j^i) = E_{j_0}^i$, on aura :

$$E_{j_0}^{i*} = s - \varepsilon_2 \tag{9.2}$$

Comme dans le cas de l'étape de modifications en vue du codage de un bit, nous effectuons la modification qui minimise les moindres carrés (voir paragraphe 13.1). Ceci revient à prendre les coefficients en paquets d'ondelettes de N_i, $C_i^*(k)$ tels que

$$C_i^*(k) = \sqrt{E_i^*}\frac{C_i(k)}{\sqrt{E_i}} \tag{9.3}$$

Relation entre les deux coefficients

La première modification implique que $\sum_j E_j^{i*} = s + \varepsilon_1$. L'énergie minimale $E_{j_0}^i$ est augmentée et dans le pire des cas (quand cette énergie est maximale) on aura une énergie $E_{j_0}^{*i} = \frac{s+\varepsilon_1}{4}$. Or la deuxième condition de sécurité doit être respectée, on a donc

$$\frac{s+\varepsilon_1}{4} \leq s - \varepsilon_2 \tag{9.4}$$

ce qui s'écrit aussi

$$\varepsilon_1 + 4\varepsilon_2 \leq 3s \tag{9.5}$$

Le couple de coefficients $(\varepsilon_1, \varepsilon_2)$ est donc compris dans le domaine du plan défini par les trois inéquations suivante :

$$\begin{cases} \varepsilon_1 \geq 0 \\ \varepsilon_2 \geq 0 \\ \varepsilon_1 + 4\varepsilon_2 \leq 3s \end{cases} \tag{9.6}$$

Prendre $\varepsilon_1 = 0$ ou $\varepsilon_2 = 0$ reviendrait à ne pas faire les modifications proposées.

On veut trouver un couple de vecteurs strictement positifs, qui respecte l'équation 9.5, qui stabilise la base et qui ne dégrade pas trop l'image. C'est ce que nous allons faire dans le prochain paragraphe.

9.2 Compromis stabilisation/invisibilité

9.2.1 Stabilisation

Nous avons testé le nombre de noeuds stables pour les images Barbara, Lenna et Bateau et pour 4 valeurs du couple $(\varepsilon_1, \varepsilon_2)$. L'attaque permettant de jauger la stabilité de la meilleure base est par exemple une compression JPEG de 30% de qualité. Le seuil le sélection de la meilleure base est pris à $10^{-6.15}$.

Les quatre couples $(\varepsilon_1, \varepsilon_2)$ sont choisis comme décrit ci dessous :

– Le premier couple est pris à $(0,0)$, il n'y a pas de modifications, on ne fait pas l'étape de stabilisation. Les résultats sur ce couple serviront de référence.

- Le deuxième couple est $(3s, 0)$, ε_1 est maximum, les noeuds d'énergie comprise entre s et $4s$ sont tous augmentés à la valeur $4s$. On ne touche pas au noeuds fils de trop grande énergie.
- Le troisième couple représente une valeur intermédiaire pour ε_1 : $(\varepsilon_1, \varepsilon_2) = (s, s/2)$, ε_2 est pris maximum pour ε_1 fixé selon la formule 9.5.
- Enfin, le dernier couple permet d'étudier la robustesse du système selon l'influence de ε_2 : $(\varepsilon_1, \varepsilon_2) = (0, 3s/4)$. On ne modifie que les noeuds fils de trop grande énergie.

Le tableau 9.1, montre les résultats en nombre de noeuds instables pour les différentes images et les différents couples de coefficients. Le tableau suivant contient en pourcentage les améliorations que chaque quantification a produit sur le nombre de noeuds instables. Le tableau 9.3 montre le résultat que produisent ces modifications sur le pourcentage final de noeuds stables.

TAB. 9.1 – Nombre de noeuds instables

$(\varepsilon_1, \varepsilon_2)$	Barbara	Lenna	Caméra
$(0, 0)$	231	712	857
$(3s, 0)$	246	642	766
$(s, s/2)$	203	661	778
$(0, 3s/4)$	210	628	785

TAB. 9.2 – Améliorations sur le nombre de noeuds instables

$(\varepsilon_1, \varepsilon_2)$	Barbara	Lenna	Caméra
$(3s, 0)$	6%	-10%	-11%
$(s, s/2)$	-12%	-7%	-9%
$(0, 3s/4)$	-9%	-12%	-8%

TAB. 9.3 – Pourcentage de noeuds stables

$(\varepsilon_1, \varepsilon_2)$	Barbara	Lenna	Caméra
$(0, 0)$	96.8%	84.5%	83.5%
$(3s, 0)$	96.6%	86%	85.3%
$(s, s/2)$	97.2%	85.6%	85.1%
$(0, 3s/4)$	97.1%	86.3%	85%

Le tableau 9.2 montre que les différentes images n'ont pas du tout le même comportement face aux différents cas étudiés. Par exemple, la première stabilisation est très bénéfique pour l'image Caméra alors qu'elle dégrade les performances obtenues pour l'image Barbara. Pour l'image Lenna, les meilleures performances sont obtenues lorsque le coefficient ε_2 est maximum, forçant ε_1 à zéro (couple 4). Pour ce couple les résultats obtenus pour les deux autres images sont moyens.

Pour ces différents cas, le comportement de la qualité des images a été étudié en PSNR. Le tableau 9.4 présente les résultats obtenus, ils sont tous de qualité acceptable (de PSNR supérieur à 35 dB).

TAB. 9.4 – PSNR des images stabilisées (dB)

$(\varepsilon_1, \varepsilon_2)$	Barbara	Lenna	Caméra
$(3s, 0)$	36.5	39.1	37.1
$(s, s/2)$	46.9	49.6	47.6
$(0, 3s/4)$	45.1	48	45.8

Nous pouvons constater que l'étape de stabilisation peut améliorer les résultats (voir tableau 9.3) et n'entraîne pas trop de dégradations de la qualité des images (voir le tableau 9.4). Globalement, le couple de coefficients qui convient le mieux à notre problème est le troisième : $(\varepsilon_1, \varepsilon_2) = (s, s/2)$. C'est ce couple que nous utiliserons en pratique.

Dans le paragraphe suivant nous allons étudier plus précisément les distorsions que le choix du couple de coefficients entraîne sur les images. Puis nous montrerons les améliorations que l'étape de stabilisation permet pour l'ensemble des attaques test présentées dans le chapitre 8.

9.2.2 Invisibilité

Nous avons étudié la visibilité de cette étape pour l'image Bateau et pour un seuil de sélection de la meilleure base de $10^{-6.15}$. La figure 9.1 montre les résultats obtenus en termes de $PSNR$ après stabilisation. Le coefficient ε_1 varie de 0 à $3s$ et ε_2 varie de 0 à son maximum. Nous avons superposé sur le graphique le plan à $40dB$ que l'on considère comme une limite de visibilité. Il ne faut pas que cette étape dégrade trop l'image, elle constitue un préliminaire au tatouage qui fournira l'essentiel des dégradations.

On remarque que les distorsions sont plus sensibles au coefficient ε_1 qu'à ε_2. Dans le premier cas on ajoute de l'énergie à des paquets considérés d'énergie significative, il y aura des distorsions. Dans le deuxième cas, on fait l'opposé : on diminue le gain en énergie de paquets contenant peu d'information. Les coefficients les plus petits sont encore diminués. Cette opération est donc beaucoup moins coûteuse en terme de qualité.

Dans la suite, on prendra toujours ε_2 maximum selon la relation 9.5. Avec cette valeur de ε_2, la surface représentant les valeurs de la distorsion devient une courbe présentée figure 9.2. On remarque qu'un maximum est atteint pour $\varepsilon_1 = 2s/3$ et que l'image est considérée de bonne qualité pour toutes valeurs de $\varepsilon_1 < 2s$.

Les figures 9.3 et 9.4 présentent la même étude sur l'image Lenna. Les valeurs du PSNR sont un peu meilleures que celles obtenues pour Bateau. Les courbes ont la même forme dans les deux cas. On retrouve le maximum du $PSNR$ pour $\varepsilon 1 = 2s/3$.

En conclusion, on fixera le paramètre ε_1 proche de s (valeur que l'on a choisi au paragraphe 9.2). ε_2 est pris maximum selon l'inéquation 9.5. On considérera par la suite

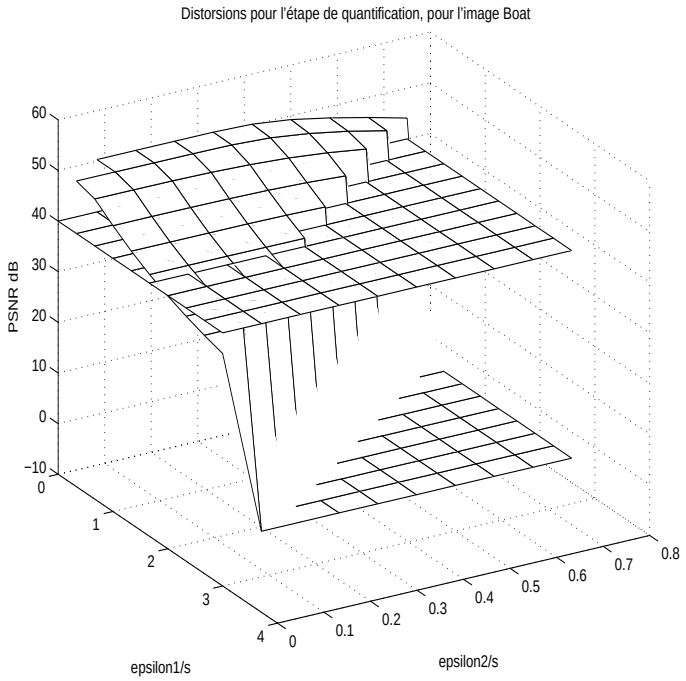


FIG. 9.1 – Distorsions entraînées par l'étape de stabilisation pour l'image Bateau

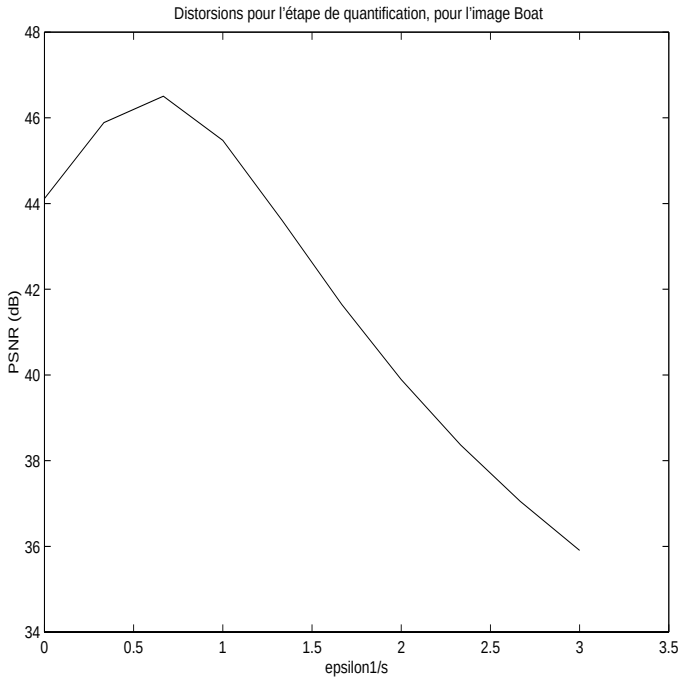


FIG. 9.2 – Distorsions entraînées par l'étape de stabilisation pour l'image Bateau

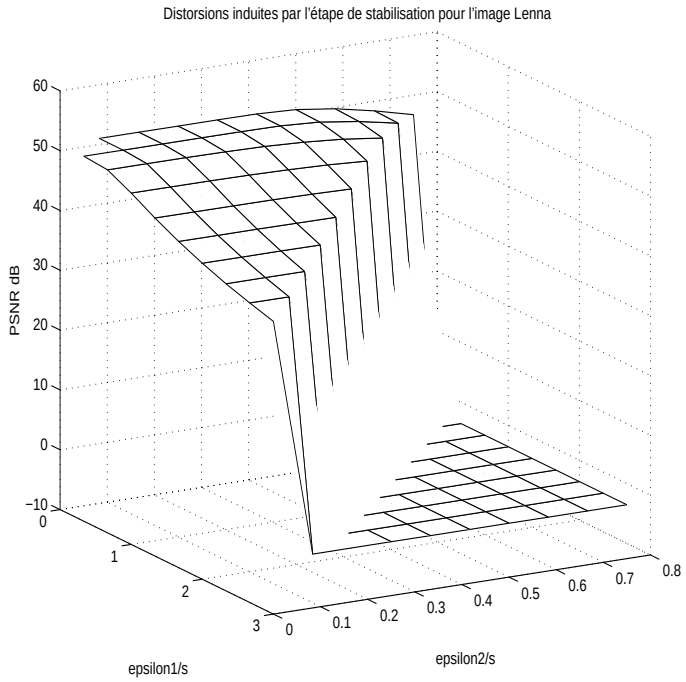


FIG. 9.3 – Distorsions entraînées par l'étape de stabilisation pour l'image Lenna

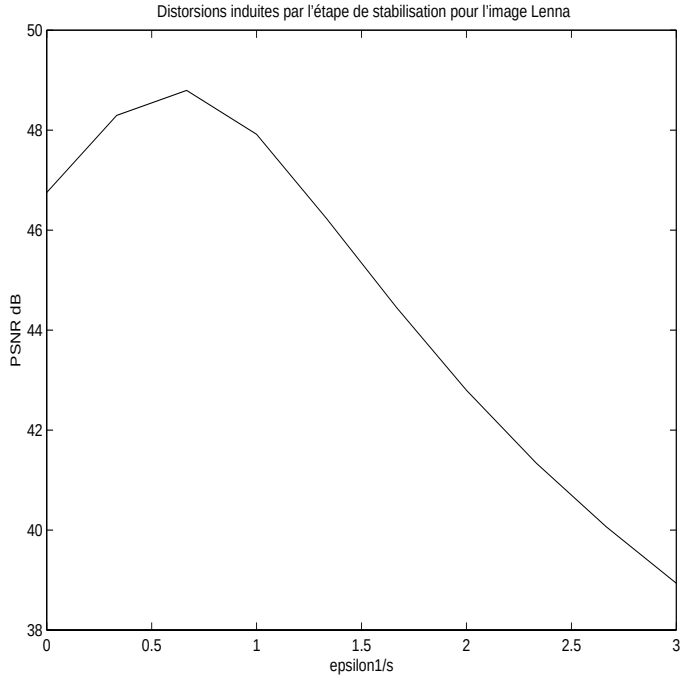


FIG. 9.4 – Distorsions entraînées par l'étape de stabilisation pour l'image Lenna

que cette étape de stabilisation de la structure de la base n'apporte pas de distorsions gênantes sur l'image.

9.3 Résultats

On prend comme image test l'image Barbara. On stabilise la meilleure base obtenue avec un seuil de sélection $s = 10^{-6.15}$. $\varepsilon_1 = s$, et ε_2 est maximum $\varepsilon_2 = s/2$. L'image obtenue est représentée avec l'image originale figure 9.5. Il n'y a pas de modifications visibles entre les deux images. Le PSNR est égal à $46.9dB$.

FIG. 9.5 – Image Barbara originale et après étape de stabilisation

La figure 9.6 présente les résultats en terme de stabilité que l'on obtient avec et sans cette étape. Les ordonnées de l'image donnent le nombres de noeuds de la meilleure base stables après une attaque. Les abscisses sont le numéro des attaques Stirmark comme présenté au chapitre 8. La courbe avec des $\triangle$ est obtenue pour une base non stabilisée et pour un seuil de sélection de 10^-6. La courbe avec des o est obtenue pour la base stabilisée présentée ci-dessus. Les seuils étant très proches, nous pouvons comparer les deux courbes. La courbe 9.7 présente les mêmes résultats en pourcentage. On remarque que la méthode de stabilisation améliore les résultats pour les attaques qui ne dégradent pas trop l'image (les cropping et les compression JPEG situés en début et fin de l'axe des abscisses). Pour les autres attaques, cette étape dégrade les résultats.

9.4 Conclusion

Nous avons défini et mis en oeuvre dans ce paragraphe une étape supplémentaire permettant d'accroître les performances de notre algorithme à certaines attaques. Nous avons en particulier étudié les distorsions que cette modification supplémentaire induit sur l'image et nous avons ainsi déterminé les valeurs des coefficients pour lesquels ces distorsions sont négligeables ou imperceptibles. En ce qui concerne la stabilité, les comportements des différentes images semblent apporter des résultats relativement hétéroclites. Nous nous contenterons par la suite de fixer la valeur du couple de paramètres $(\varepsilon_1, \varepsilon_2)$ à la valeur donnant globalement les meilleurs résultats c'est à dire $(s, s/2)$.

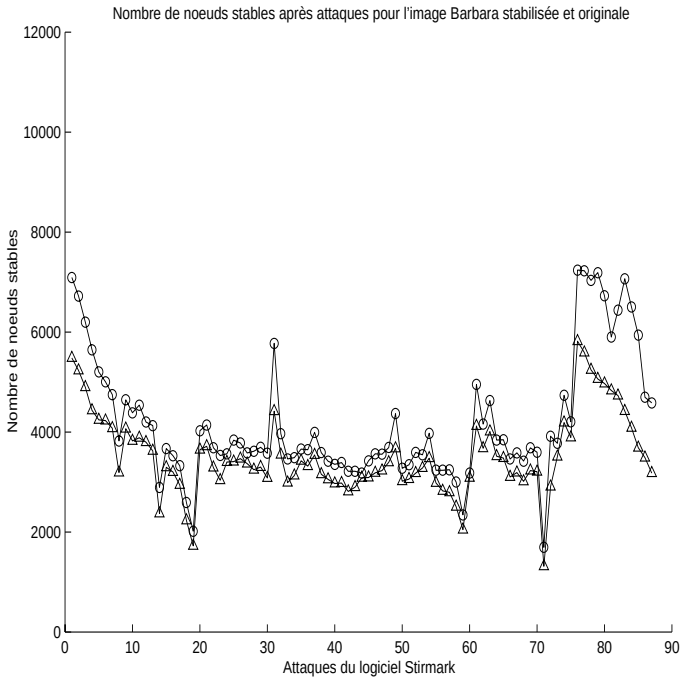


FIG. 9.6 – Nombres de noeuds stables après attaques pour l'image Barbara stabilisée ("o") et originale ($\triangle$)

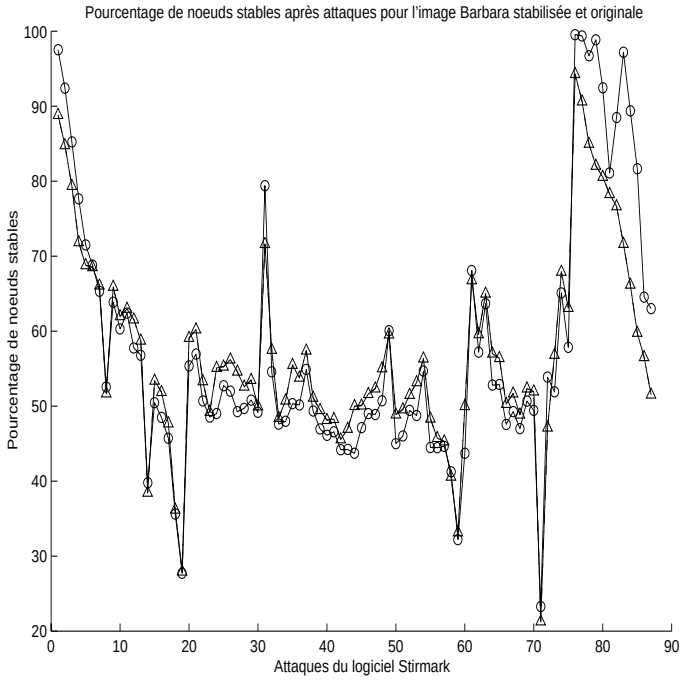


FIG. 9.7 – Pourcentages de noeuds stables après attaques pour l'image Barbara stabilisée ("o") et originale ($\triangle$)

Chapitre 10

Optimisation de la stabilité de la meilleure base : recherche du seuil de sélection optimum

Nous avons présenté dans le paragraphe 5.3 le critère permettant de sélectionner la meilleure base. L'algorithme de sélection fait intervenir un seuil s dont la valeur fixe la structure de la meilleure base. Le tatouage étant porté par cette structure, nous avons vu que sa stabilité était une contrainte forte de la méthode. Une étude du comportement de la structure de la meilleure base face à diverses attaques a été présentée au chapitre 8. Nous avons vu à cette occasion que différents choix du seuil donnaient des résultats variés sur la stabilité de la base.

Dans ce chapitre nous nous proposons de trouver la valeur du seuil s telle que la base sélectionnée soit la plus stable possible. Nous commencerons par rappeler les premières contraintes inhérentes au choix de s. Puis nous définirons une condition suffisante de la stabilité de la base en fonction du paramètre s et de l'énergie des paquets d'ondelettes avant et après attaque. Comme on n'a aucune information sur les attaques auxquelles doit résister la structure, on ne peut pas connaître le comportement des énergies après ces attaques. La suite de notre travail consiste à modéliser ce comportement par apprentissage paramétrique sur l'ensemble des coefficients attaqués par l'ensemble des attaques décrites au paragraphe 8.2. Le critère de stabilité peut alors être optimisé. Nous donnerons les résultats obtenus sur le critère et sur la détermination de seuils de sélection de meilleure base. Puis nous montrerons les résultats des améliorations de la stabilité que ces choix permettent.

10.1 Rôle du seuil de sélection de la meilleure base

Nous avons vu paragraphe 5.3 le mécanisme de sélection de la meilleure base en fonction de l'arbre des énergies des coefficients en paquets d'ondelettes et du seuil s. Les noeuds sélectionnés dans la meilleure base sont ceux qui ont une énergie supérieure au seuil et dont un fils au moins à une énergie inférieure à ce seuil. Pour pouvoir réaliser le

tatouage, la structure de la meilleure base doit posséder des caractéristiques entraînant les deux contraintes sur s que nous rappelons ci-dessous :

- Le seuil doit être assez petit pour sélectionner un nombre suffisant de paquets. La structure de la base sera alors suffisamment complexe pour permettre l'encodage d'une marque de taille correcte. En notant $\bar{e} = \sup_i c_i$, on doit prendre $s < \bar{e} - \varepsilon$, où ε est un coefficient à déterminer et c_i représente l'énergie du noeuds N_i.
- La valeur du seuil de sélection doit être assez importante pour au moins deux raisons. D'abord, il faut sélectionner des composantes d'énergie significative de l'image (c'est un des principes de notre méthode de tatouage). D'autre part, la valeur de s doit être assez grande pour éviter la sélection d'un trop grand nombre de paquets du dernier niveau de décomposition (ces paquets ne peuvent pas être modifié, ils ne sont pas concernés par le tatouage). Si $\underline{e} = \inf_i c_i$, on prendra donc $s > \underline{e} + \varepsilon$.

Nous avons vu sur des tests numériques (voir le paragraphe 8.3) que du choix du seuil dépend la stabilité de la base. Notre objectif est d'optimiser un critère de stabilité de la base selon s. La valeur s_{opti} qui optimise le critère sera cherchée dans un intervalle $[\underline{e} + \varepsilon, \bar{e} - \varepsilon]$ déterminé grâce aux deux contraintes rappelées ci-dessus.

10.2 Définition d'un critère de stabilité de la meilleure base

10.2.1 Condition suffisante de stabilité de la meilleure base

Notations

Notons $I(A)$ l'ensemble des indices de tous les noeuds de l'arbre de décomposition en paquets d'ondelettes d'une image A. On définit les ensembles $J(A)$ et $K(A)$ tels que $i \in J(A)$ si et seulement si $c_i > s$ et $K(A)$ est le complémentaire de $J(A)$ dans $I(A)$.

Stabilité des ensembles J et K

Nous avons vu au paragraphe 8.1, la définition de la stabilité de la base et des noeuds qui la composent. Pour les ensembles J et K, cette définition devient :

Définition 5 *Si après une attaque sur A conduisant à une image A', on a $J(A') = J(A)$ alors J est dit stable pour cette attaque. J sera stable à un ensemble d'attaques s'il est stable pour chacune.*

Il est évident que la stabilité de J entraîne directement celle de K et réciproquement.

Condition suffisante de stabilité de la meilleure base

Si l'arbre de décomposition de l'image est stable, c'est à dire si J et K sont stables, les noeuds composant la base B sont *a fortiori* stables, la base est alors stable. On a donc la condition suffisante suivante : Si J est stable la base B est stable.

Stabilité à une attaque donnée

Soit d_i l'énergie du noeud i après une attaque. Alors la condition de stabilité des deux ensembles J et K s'écrit :
- $c_i > s \Rightarrow d_i > s$
- $c_i \leq s \Rightarrow d_i \leq s$

10.2.2 Critère de stabilité de la meilleure base

Les conditions de stabilité définies ci dessus peuvent être exprimées, avec les mêmes notations :

$$(c_i > s \Rightarrow d_i > s \text{ et } c_i < s \Rightarrow d_i < s) \Rightarrow (\text{la base est stable}) \tag{10.1}$$

Ainsi la condition suffisante de stabilité est optimale (car vérifiée sur un nombre maximal de noeuds) si l'on minimise le critère suivant :

$$C_r(s) = -\sum_{i \in I} (sgn(c_i - s)(sgn(d_i - s)) \tag{10.2}$$

où sgn représente la fonction «signe» : $sgn(x) = \frac{x}{|x|}, sgn(0) = 0$.
On cherche donc à minimiser le nombre de coefficients pour lesquels : $c_i - s$ et $d_i - s$ sont de signes opposés.

Afin de travailler dans un cadre plus général et de permettre ainsi de trouver un meilleur optimum, nous allons rechercher un *couple* de seuils (λ, λ') au lieu d'un unique coefficient s. Le seuil λ sera le seuil de sélection de la meilleure base utilisé à l'implémentation de la marque, λ' sera le seuil utilisé à la détection de la marque. Le critère devient :

$$C_r(\lambda, \lambda') = -\sum_{i \in I} (sgn(c_i - \lambda)(sgn(d_i - \lambda')) \tag{10.3}$$

10.3 fournit un critère de stabilité C_r, dépendant d'un couple de seuils. Ce critère est exprimé en fonction de toutes les énergies des noeuds de l'arbre de décomposition de l'image en paquets d'ondelettes, avant et après attaque. Or, nous voulons minimiser C_r sans savoir *a priori* quelle attaque l'image a subie. Nous devons donc modéliser les modifications des énergies des coefficients en paquets d'ondelettes après une attaque quelconque.

10.3 Modélisation stochastique

Nous considérons le modèle stochastique suivant : soit Ω l'ensemble d'événements élémentaires composé de «toutes les attaques identifiées» (par exemple les attaques implémentées dans *Stirmark*). Notre triplet de probabilité est alors : $(\Omega, \mathcal{B}, \mathcal{P})$ où $\mathcal{B}$ est

l'algèbre naturelle associée à Ω, et $\mathcal{P}$ est la probabilité uniforme (toutes les attaques sont équiprobables). Pour chaque index $i \in I$, le coefficient d'énergie du paquet d'ondelettes d_i est une variable aléatoire dont la distribution F_i est déterminée par le résultat de l'action de toutes les attaques possibles sur le coefficient c_i.

Nous considérons la version stochastique déduite de 10.3 :

$$S(\lambda, \lambda') = -\sum_{i \in I} \phi(c_i - \lambda) sgn(d_i - \lambda') \tag{10.4}$$

où ϕ est une fonction C^∞ qui approxime la fonction sgn, par exemple la fonction arctangente. L'usage de ϕ stabilise l'étape d'optimisation.

Pour simplifier le problème, nous minimiserons $B(\lambda, \lambda') = E(S(\lambda, \lambda'))$ où E est l'espérance mathématique.

Comme annoncé au paragraphe 10.1 nous restreindrons la recherche du couple de seuil (λ, λ') à un carré Λ. Nous prendrons $\Lambda = [\underline{e}, \overline{e}]^2$ avec $\underline{e} = \inf_i c_i$ et $\overline{e} = \sup_i c_i$. Cette restriction est une version «diminuée» des contraintes rappelées au paragraphe 10.1. Elle permet de plus de bien poser le problème sinon $(\lambda,\ \lambda') = (0, 0)$ et $(\lambda,\ \lambda') = (\infty, \infty)$ seraient les solutions dégénérées de notre problème.

Les valeurs de $sgn(d_i - \lambda')$ sont des variables aléatoires de Bernoulli, avec $sign(d_i - \lambda') = 1$ avec la probabilité $F_i(\lambda')$ et $sign(d_i - \lambda') = -1$ avec la probabilité $1 - F_i(\lambda')$. On obtient l'espérance suivante :

$$B(\lambda, \lambda') = \sum_{i \in I} \phi(c_i - \lambda)(1 - 2F_i(\lambda')) \tag{10.5}$$

Si les F_i sont C^2, alors $B(\lambda, \lambda')$ l'est[1], et son minimum peut être trouvé par une méthode classique comme la plus forte pente. Ce calcul nécessite cependant la connaissance des F_i, problème que nous abordons ensuite : L'objectif des paragraphes suivants sera d'approximer la fonction de densité de probabilité f_i par une fonction Gamma (nous expliquerons les raisons de ce choix). Les paramètres de cette fonction seront estimés sur un ensemble d'apprentissage composé de l'ensemble des énergies des paquets d'ondelettes de trois images attaquées par l'ensemble des attaques contenues dans le logiciel Stirmark présentées au paragraphe 8.2.

[1]Bien qu'il y ait un nombre fini d'attaques dans Stirmark, nous considèrerons cependant que les F_i possèdent une fonction de densité. En effet, différents paramètres (e.g. le taux de compression JPEG) peuvent être rendus continus.

10.4 Apprentissage paramétrique

10.4.1 Distributions empiriques de l'énergie des paquets attaqués

Ensemble d'apprentissage, attaques Notre ensemble d'apprentissage est constitué des trois images Lenna, Barbara et Bateau.

L'ensemble d'attaques est constitué par les attaques du logiciel Stirmark décrites paragraphe 8.2 auxquelles s'ajoute un cropping de 75%.

Exemples de distributions empiriques Les figures 10.1 et 10.2 représente les distributions empiriques obtenues pour les trois images pour différentes localisations des noeuds dans l'arbre de décomposition et pour les 89 attaques implémentées dans le logiciel Stirmark. Les résultats obtenus pour l'image Barbara sont représentés sur les graphiques de gauches, ceux de Lenna sont au milieu et ceux de Bateau à droite.

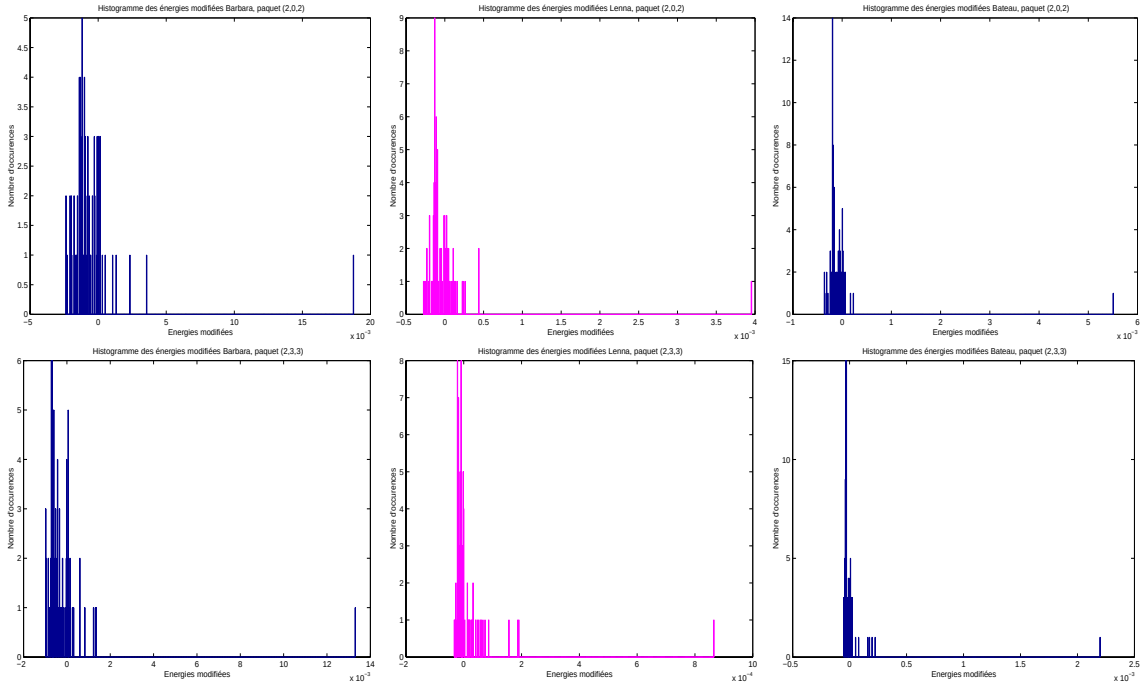


FIG. 10.1 – Distributions empiriques des énergies des coefficients en paquets d'ondelettes attaquées.

Les deux premiers résultats sont obtenus pour des paquets de profondeur 2 et pour des moyennes et hautes fréquences. Les suivants concernent des paquets de profondeurs 3 et des moyennes et hautes fréquences. Les cinquièmes résultats sont obtenus pour une profondeur p de 6 et en moyenne fréquences. Les dernières figures représentent les résultats pour le dernier niveau et des hautes fréquences.
Les énergies présentées ont été translatées de leurs valeurs originales (on a représenté

$d'_i = d_i - c_i$). On peut remarquer que la majorité des attaques fait baisser l'énergie du paquet considéré et qu'une attaque la fait considérablement augmenter. Les répartitions des énergies des trois différentes images se ressemblent. On peut toutefois noter que les modifications semblent beaucoup plus violentes pour l'image Barbara.

10.4.2 Choix de la fonction de distribution

Après avoir calculé les distributions empiriques des d_i, nous approximons alors les f_i (densité de probabilité des énergies modifiées d_i) en utilisant des versions translatées de la distribution Gamma. La densité approximante f_i est calculée selon :

$$f_i(x) = \gamma(x - a - c_i)^{b-1} e^{-c(x-a-c_i)} H(x - a - c_i) \tag{10.6}$$

où $\gamma = \frac{c^b}{\Gamma(b)}$ et H est la fonction de Heaviside. a, b, c sont les paramètres à estimer.

Le choix de la distribution Gamma translatée est faite sur la base de l'observation des distributions empiriques obtenues (figures 10.1et10.2) et de considérations «semi-heuristiques». En particulier, si nous considérons que nous modélisons l'action des attaques comme l'addition d'un bruit blanc gaussien sur les coefficients des paquets, alors on peut montrer que les énergies sont distribuées selon une fonction chi-square, qui est un cas particulier de la distribution Gamma. De plus, la fonction Gamma est stable par combinaisons linéaires, ce qui correspond aux opérations qui ont lieu quand on change de niveau dans l'arbre de décomposition.

10.4.3 Estimation des paramètres de la fonction densité de probabilité

10.4.3.1 Classes d'apprentissage

Pour chaque noeud N_i, on doit estimer les trois paramètres de f_i, c'est à dire (a_i, b_i, c_i) pour les 89 attaques et les trois images. Or on a : $(4^{p+1} - 1)/3$ noeuds dans l'arbre où p est la profondeur maximale. Le nombre de paramètres à estimer dans notre cas sera donc de 87381 triplets ($p = 8$). Pour réduire la complexité du problème, il est indispensable de regrouper certains noeuds. Il faut donc choisir un découpage de l'arbre de décomposition en classes dans lesquelles tous les noeuds sont supposés avoir la même loi f_i. Ce découpage servira aussi à obtenir les classes d'apprentissages. Le comportement des coefficients d_i étant différent selon la profondeur de l'arbre (voir les figures 10.1 et 10.2), nous allons conserver le découpage en différentes profondeurs, c'est à dire avoir des classes différentes par niveau. A l'intérieur de chaque niveau de résolution, nous regroupons les noeuds selon leurs fréquences en 16 classes selon le schéma présenté à la figure 10.3.

Les deux premiers niveaux de l'arbre ne sont pas considérés (ils sont supposés d'énergie très supérieure au seuil donc stables). On a ainsi réduit le problème à l'estimation de $16 \times 7 = 112$ triplets de paramètres à estimer.

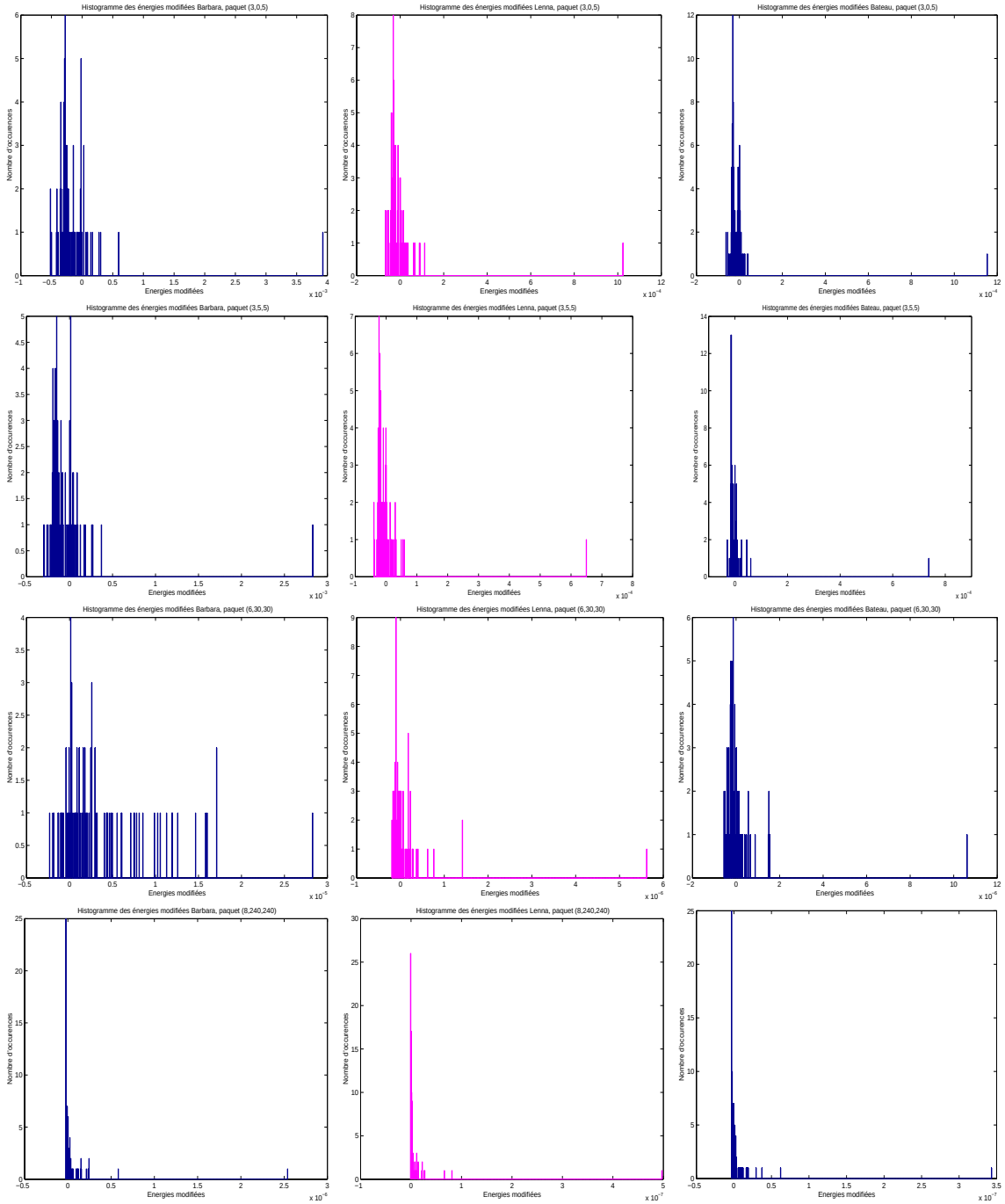


FIG. 10.2 – Distributions empiriques des énergies des coefficients en paquets d'ondelettes attaquées.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

FIG. 10.3 – Schéma du découpage d'un niveau de l'arbre, regroupement des noeuds

Afin de pouvoir travailler sur les trois images en même temps, nous translaterons les énergies d_i selon $d'_i = d_i - c_i$. Les graphiques 10.1 et 10.2 montrent qu'alors, conformément à nos suppositions, les répartitions des énergies se ressemblent.

Nous allons maintenant présenter deux méthodes d'estimation : le maximum de vraisemblance et la méthode des moments. Nous allons appliquer ces méthodes à notre problème d'estimation des paramètres de fonctions Gamma translatées, nous comparerons ensuite les deux méthodes sur des simulations. Enfin, nous donnerons les résultats obtenus pour l'estimation des valeurs des énergies modifiées par les attaques.

10.4.3.2 Estimation par maximum de vraisemblance

Soit $\theta = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. L'optimum $\hat{\theta}$ est défini par : $\hat{\theta} = Argmax(f(\mathcal{X}/\theta))$ où $\mathcal{X}$ est l'ensemble des éléments d'une classe d'apprentissage : $\mathcal{X} = \{x_1, x_2, ..., x_n\}$

$$f(\mathcal{X}/\theta) = \prod_{k=1}^{n} \gamma.(x_k - a)^{b-1} exp(-c(x_k - a)).H(x_k - a) \tag{10.7}$$

où $\gamma = \frac{c^b}{\Gamma(b)}$. On a donc

$$\hat{\theta} = Argmax(\sum_{k=1}^{n} b\log(c) - \log(\Gamma(b)) + (b-1)\log(x_k - a) - c(x_k - a)) \tag{10.8}$$

La condition nécessaire du premier ordre ($(\frac{\partial f(\mathcal{X}/\theta)}{\partial \theta})_{\theta=\hat{\theta}} = 0$) implique :

$$\begin{cases} (\hat{b}-1)\sum_k \frac{1}{x_k-\hat{a}} - n\hat{c} = 0 \\ n\log(\hat{c}) - n\frac{\Gamma'(\hat{b})}{\Gamma(\hat{b})} + \sum_k(\log(x_k-\hat{a})) = 0 \\ n\frac{\hat{b}}{\hat{c}} - \sum_k(x_k-\hat{a}) = 0 \end{cases} \tag{10.9}$$

avec $n = |\mathcal{X}|$ le cardinal de la classe d'apprentissage.
Posons $u = \frac{\hat{b}}{\hat{c}}$. On a le système suivant :

$$\begin{cases} \hat{a} = m - u \\ \hat{b} = \frac{Su}{Su-n} \\ \hat{c} = \frac{S}{Su-n} \end{cases} \tag{10.10}$$

avec $m = \frac{1}{n}\sum_k x_k$ et $S = \sum_k \frac{1}{x_k-m+u}$.

Le paramètre d'estimation u est obtenu en résolvant numériquement l'équation suivante sur $\mathbb{R}$:

$$log(S) - log(Su-n) - \Psi(\frac{Su}{Su-n}) + \frac{1}{n}\sum(x_k - m + u) = 0 \tag{10.11}$$

où Ψ est la fonction Digamma $\frac{\Gamma'}{\Gamma}$.
On en déduit ensuite $\hat{a}, \hat{b}, \hat{c}$.

La résolution de u étant numérique, on ne peut pas calculer littéralement le biais de l'estimateur. Nous verrons au paragraphe 10.4.3.4 que les résultats de l'estimation des coefficients (a, b, c) sur des signaux simulés ne sont pas bons pour le cas b petit. Nous présentons maintenant une estimation de ces coefficients par la méthode des moments.

10.4.3.3 Estimation par la méthode des moments

La méthode des moments consiste à exprimer les coefficients recherchés (dans notre exemple a b c) par les moments de la densité de probabilité. Prenons les mêmes notations qu'au paragraphe précédent. m est l'espérance de x_k, V est la variance et μ_3 le moment d'ordre 3. Nous avons les relations suivantes :

$$\begin{cases} m = a + \frac{b}{c} \\ V = \frac{b}{c^2} \\ \mu_3 = \frac{2b}{c^3} \end{cases} \tag{10.12}$$

Ce système de trois équations à trois inconnues admet une unique solution présentée ci-dessous :

$$\begin{cases} a = m - \frac{2V^2}{\mu_3} \\ b = \frac{4V^3}{\mu_3^2} \\ c = \frac{2V}{\mu_3} \end{cases} \tag{10.13}$$

On estimera les différents moments sur n réalisations x_k de f par :

$$\begin{cases} m = \frac{1}{n}\sum_i x_i \\ \sigma^2 = \frac{1}{n}\sum_i (x_i - \hat{\hat{m}})^2 \\ \mu_3 = \frac{1}{n}\sum_i (x_i - \hat{\hat{m}})^3 \end{cases} \tag{10.14}$$

Bien que cet estimateur soit biaisé (les estimations de σ^2 et μ_3 le sont), nous verrons dans le paragraphe suivant sur des simulations qu'il nous convient mieux que le maximum de vraisemblance.

10.4.3.4 Comparaisons des méthodes

Dans ce paragraphe, nous allons comparer les deux méthodes d'estimation présentées ci dessus sur des simulations.

On génère un ensemble de cardinal n de réalisations de $\mathcal{X}$, suivant la loi Gamma et on teste les deux méthodes d'estimations des paramètres (a, b, c) sur ces signaux simulés pour des valeurs «moyennes» et «extrêmes» de b et c.

Le tableau 10.1 présente les résultats de trois tests de simulation. Pour ces tests, le nombre de réalisation n est fixé à 1000.

TAB. 10.1 – Résultats des estimations sur des signaux simulés

(a, b, c)	Maximum de vraisemblance	Méthode des moments
$(10, 5, 3)$	$(11.21, 4.11, 3.26)$	$(11.63, 4.05, 3.21)$
$(10, .5, 3)$	$(7.54, 6.55, 0.6)$	$(10.07, 0.40, 3.52)$
$(10, 5, 0.03)$	$(10, 4.89, 0.03)$	$(10, 4.74, 0.03)$

La figure 10.4 présente les graphiques obtenus pour chacun des cas ci dessus. Les courbes de densités de probabilités sont présentées sur les histogrammes et sur les figures situées au dessous. La courbe en pointillés représente la fonction densité de probabilité obtenue par estimation par maximum de vraisemblance, la courbe en trait plein représente celle obtenue dans le cas d'une estimation par les moments, la dernière courbe montre la fonction densité de probabilité réelle. Les cas 1 et 3 donnent des résultats comparables pour les deux méthodes. Pour le cas ou b est petit, l'estimation par maximum de vraisemblance donne de très mauvais résultats. On utilisera donc pour l'estimation la méthode des moments.

10.4.3.5 Résultats des estimations sur l'ensemble d'apprentissage

La figure 10.5 présente les résultats obtenus sur les classes de l'ensemble d'apprentissage. Les distributions empiriques des énergies des paquets attaqués ainsi que la fonction densité de probabilité estimée sont représentées pour les trois images et pour différents regroupements de paquets. Le numéro des regroupement est celui indiqué sur la figure 10.3. En décrivant les graphiques de haut en bas et de gauche à droite, le

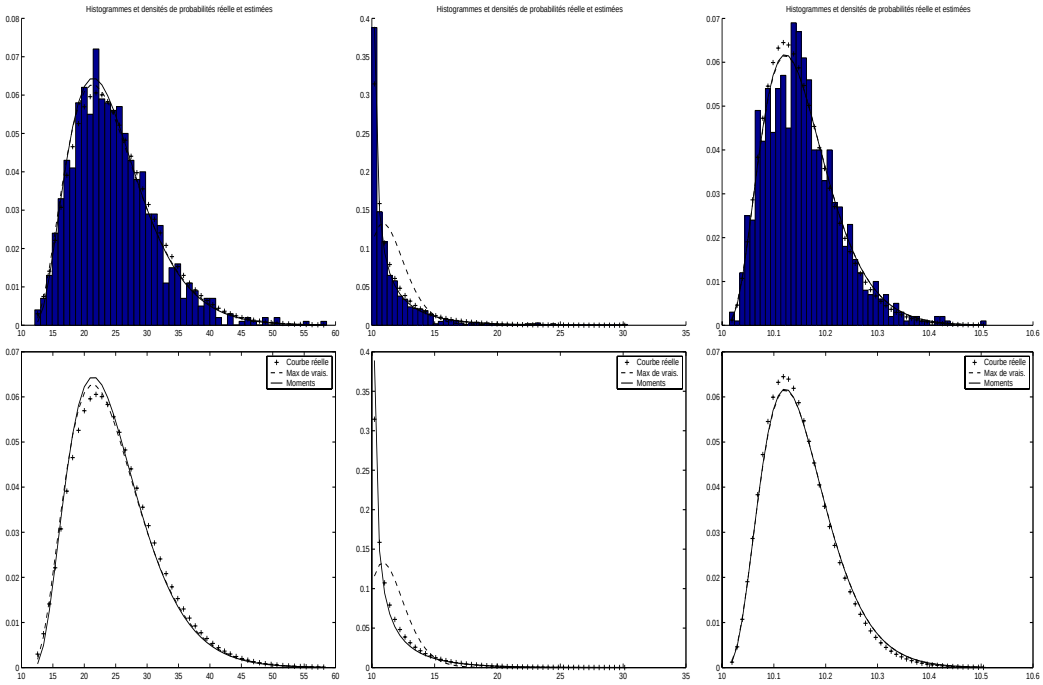


FIG. 10.4 – Comparaisons des méthodes d'estimation par maximum de vraisemblance et par la méthode des moments. Histogrammes des distributions simulées et estimations dans trois cas.

premier graphique présente les résultats pour le groupe de paquets $(2, 13)$ (profondeur 2, groupement 13) ; puis on a les groupements de paquets : $(4, 11)$, $(4, 13)$, $(5, 1)$, $(5, 15)$,$(6, 10)$,$(6, 11)$,$(6, 13)$,$(6, 5)$. On a ainsi un aperçu de tout l'arbre.

10.5 Optimisation du critère de stabilité de la base

Avec les paramètres de f_i trouvés ci dessus, on calcule le critère de stabilité pour différentes valeurs des seuils (λ, λ') pour l'image Bateau. La surface ainsi calculée est présentée à la figure 10.6 sous deux angles de représentation. On remarque tout d'abord que l'optimum trouvé est sur le bord de la surface et correspond à des grandes valeurs des seuils (couple $(10^{-5}, 10^{-5.3})$). Il semble que le choix d'un grand seuil soit alors le meilleur pour la stabilité de la base (ce choix ne nous permet pas d'insérer une marque très longue). La seconde remarque porte sur le fait que la courbe est dissymétrique : le couple optimum (λ, λ') est tel que $\lambda' < \lambda$: ceci correspond à notre observation sur les énergies empiriques qui ont tendance à diminuer. On prendra donc différents seuils pour l'implémentation et la détection de la marque.

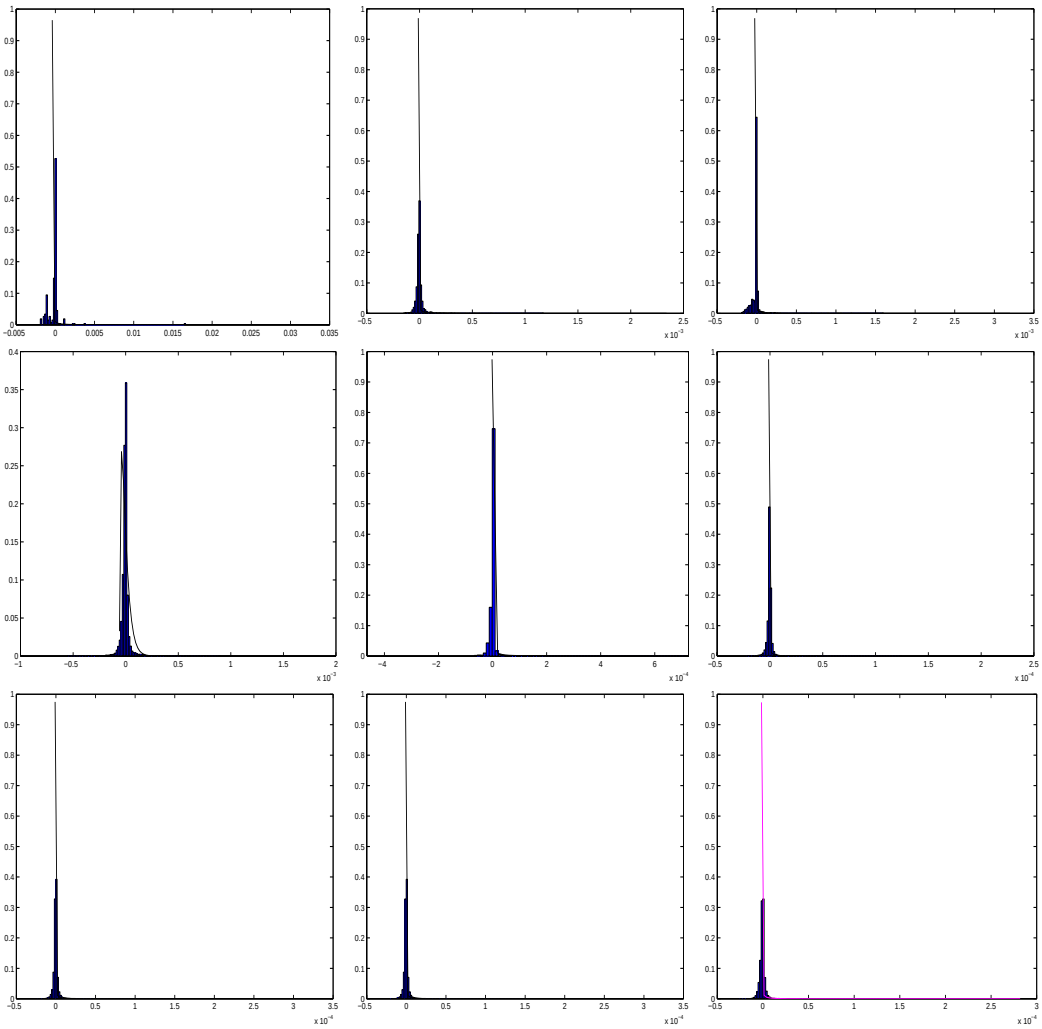


FIG. 10.5 – Distributions empiriques des énergies et densités de probabilités estimées pour les paquets respectivement de profondeurs et de numéro de regroupement : $(2, 13)$,$(4, 11)$,$(4, 13)$, $(5, 1)$, $(5, 15)$,$(6, 10)$,$(6, 11)$,$(6, 13)$,$(6, 5)$.

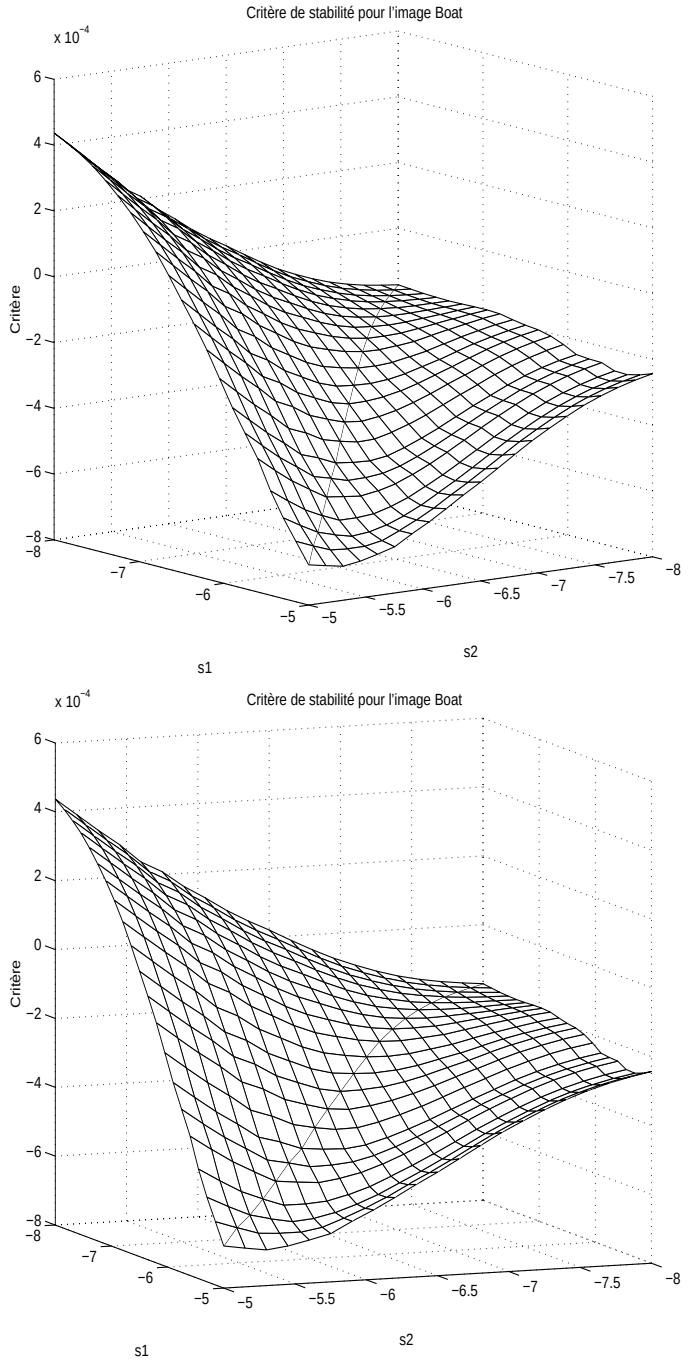


FIG. 10.6 – Critères de stabilité de la base pour l'image Bateau selon les choix du couple de seuil de sélection de la meilleure base s_1 et s_2 exprimés en puissance de 10. Présentation sous deux orientations différentes.

10.6 Résultats de l'optimisation de la stabilité de la base

La figure 10.7 présente les résultats concernant la stabilité des noeuds, obtenus pour l'image bateau. On a utilisé les même représentations qu'aux chapitres précédents. L'ordonnée du graphique représente le nombre de noeuds de la base stables et l'abscisse, les dernières transformations Stirmark.

On a représenté les résultats pour le couple optimum trouvé (voir la courbe 2 en pointillés) $C_2 = (10^{-5}, 10^{-5.3})$ et on les compare avec le résultat trouvé avec le couple correspondant symétrique $C_1 = (10^{-5}, 10^{-5})$. Les performances sont améliorées avec le choix du couple optimum sauf pour des attaques qui ne sont pas très dangereuses.

Les autres courbes correspondent aux choix de couples de seuils différents (en pointillés) comparé au choix d'un seul seuil. On a pris les valeurs : $C_3 = (10^{-6}, 10^{-6})$, $C_4 = (10^{-6}, 10^{-6.2})$, $C_5 = (10^{-7}, 10^{-7})$ et $C_6 = (10^{-7}, 10^{-7.1})$. On a le même comportement que pour le couple optimum : Le couple dissymétrique est meilleur pour les attaques les plus dangereuses.

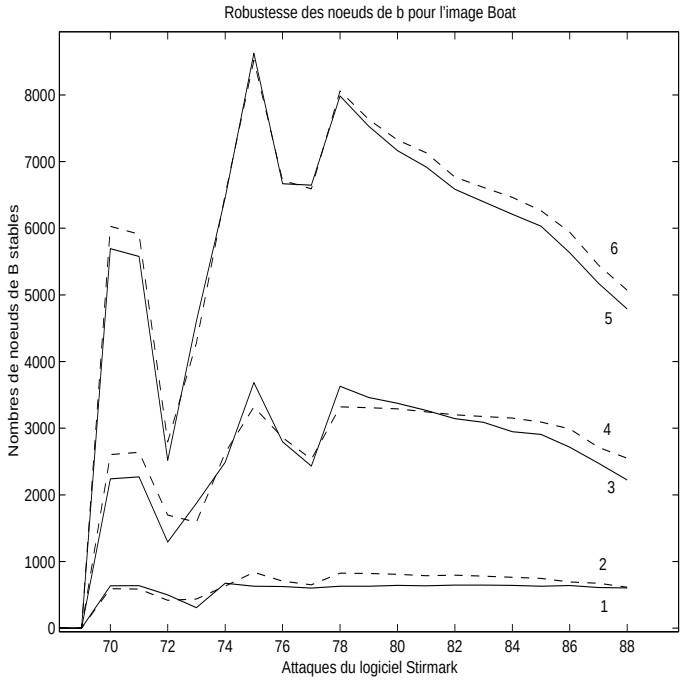


FIG. 10.7 – Nombre de noeuds de B stables pour 3 couples de seuils dissymétriques et 3 symétriques. Le choix optimum est la courbe 2 pointillés

Ce comportement est tout à fait normal. En effet, quand il n'y a pas d'attaque, toute base sélectionnée par un seuil s est forcément stable et le meilleur couple de seuils est forcément composé du seul seuil s. Quand les attaques ne sont pas trop dangereuses, on a le même résultat : c'est le couple (s, s) qui est le meilleur.

Les résultats pour toutes les attaques et pour les couples C_3 et C_4 sont présentés figure 10.8.

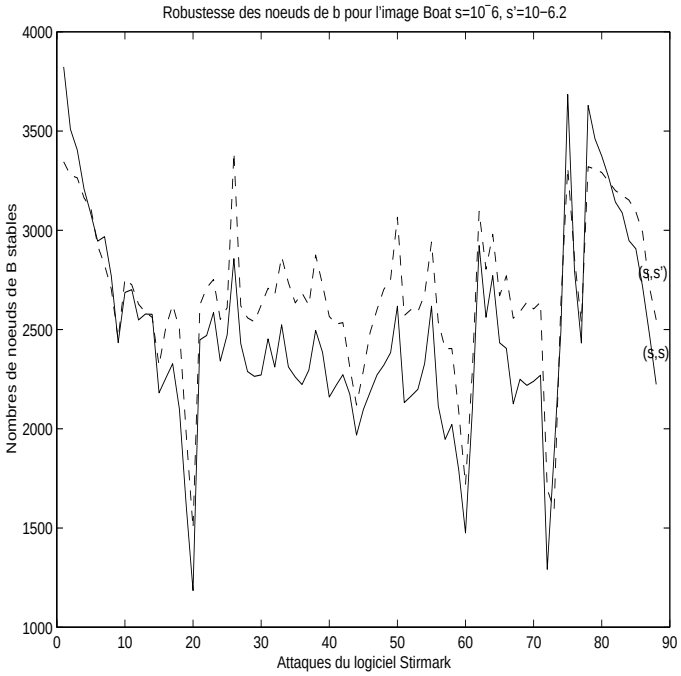


FIG. 10.8 – Nombre de noeuds de B stables pour 2 couples de seuils.

10.7 Conclusion

Nous avons présenté dans ce chapitre une méthode permettant d'optimiser un critère de stabilité de la meilleure base. Pour augmenter la généralité du problème, nous avons choisi de rechercher un couple de seuils de sélection de la meilleure base, le premier seuil caractérise la structure de la base avant attaque, le second retrouve cette structure après l'attaque. Les résultats incitent à choisir un seuil de sélection plutôt grand et nous confortent dans l'idée de considérer une procédure dissymétrique (avec deux seuils différents). Le choix de seuils optimaux peut améliorer les résultats de stabilité de la meilleure base de près de 15% après certaines attaques. S'il n'y a pas d'attaque, il est clair que nous utiliserons la procédure symétrique qui est alors la meilleure.

Lorsque nous appliquons cette méthode à notre processus de tatouage, nous supposerons que les noeuds modifiés, soit par stabilisation, soit par tatouage se comportent comme les noeuds originaux : nous appliquerons les seuils optimaux trouvés dans ce chapitre. L'application de cette étude au tatouage se fait de la manière suivante : on modifie une base sélectionnée par un seuil s comme explicité à la troisième partie, puis à la détection on utilisera soit s soit s', le seuil lui correspondant et minimisant le critère de stabilité. En effet, comme nous ne savons pas si une image test a subi une attaque, nous

commencerons par appliquer lors du processus de détection une procédure symétrique. Si la détection est négative, nous appliquerons alors la procédure asymétrique définie par le choix du seuil de sélection de la meilleure base qui minimise le critère de stabilité.

Chapitre 11

Optimisation des transformations en fonction d'un critère de qualité psychovisuel

Comme nous l'avons montré dans la partie 7, la méthode de tatouage proposée a de bonne qualité de robustesse si l'on implémente une marque assez redondante avec une force suffisante. Dans ce cas, le tatouage entraîne cependant l'apparition d'artefacts qui détériorent la qualité de l'image. Nous avons donc décidé d'utiliser un outil psychovisuel pour diminuer la distorsion entre les images originales et tatouées. Après une présentation de l'outil utilisé, nous présenterons deux méthodes : l'une très simple permet de «corriger» l'image tatouée, l'autre permet d'optimiser individuellement sur chaque paquet le paramètre ε contrôlant la force des modifications des coefficients en paquets d'ondelettes de l'image.

11.1 Détermination psychovisuelle d'une matrice contrôlant la force maximale admissible du tatouage d'une image

Nous avons présenté aux paragraphes 2.1.2 et 2.1.3, les principes de la méthode développée par F. Autrusseau *et al.* [37] qui nous permet d'obtenir le masque d'une image. Nous rappelons ci-dessous la signification de ce masque.

Pour une image donnée I de taille $(N \times N)$, le masque F est une image de même taille dont la valeur au pixel (i, j) donne l'amplitude maximale de la modification que le pixel (i, j) de l'image peut supporter sans que les dégradations résultantes ne soient perceptibles. En d'autre termes, le masque d'une image I est une matrice F telle que, si I^* est une image de même taille que I, et si la relation 11.1 est respectée pour tous les

pixels (i, j) de l'image, l'image I^* sera perceptuellement identique à I.

$$|I(i,j) - I^*(i,j)| \leq F(i,j) \tag{11.1}$$

Les figures 11.1, 11.2, 11.3 présentent des exemples de masques pour les images Bateau, Lenna et Fruit.

11.2 Correction de l'image tatouée

Dans ce paragraphe, nous allons présenter une utilisation de l'outil psychovisuel permettant d'effectuer une tâche de post-traitement sur l'image tatouée. Le principe est le suivant : une image I est très fortement tatouée, elle peut donc contenir des distorsions visibles. Nous allons corriger l'image tatouée I^* grâce à l'utilisation du masque psychovisuel. L'opération de «correction» de l'image consiste à seuiller les amplitudes des modifications par la valeur des modifications maximales admissibles données par le masque. On obtient ainsi une image tatouée de bonne qualité.

Les figures 11.4 et 11.5 montrent un exemple de cette méthode. Une marque de longueur $32 * 70$ bits est implantée dans l'image Bateau avec une force $\varepsilon = s/3$, ce qui constitue un fort marquage de l'image, la redondance étant très grande. L'image tatouée présente des distorsions visibles, le PSNR est de 20 dB. Afin de mieux représenter les distorsions (elles peuvent disparaître sur version papier) nous présentons à la figure 11.4 l'image tatouée et une image sur laquelle les amplitudes des distorsions ont été amplifiées d'un facteur 10.

L'image obtenue par correction avec le masque psychovisuel (voir la figure 11.5) est bien entendu de très bonne qualité perceptuelle (le PSNR est de 36 dB).

L'inconvénient majeur de cette méthode est que l'étape de post-traitement constitue une attaque de l'image tatouée. On ne sait donc pas si la marque est encore dans l'image corrigée. La seule façon de démontrer que cette marque est toujours présente serait de faire des tests numériques pour un grand ensemble d'images et de choix des paramètres.

La figure 11.6 représente la réponse du détecteur avant attaque et après attaque de l'image bateau corrigée. Sur cet exemple, on voit que la détection avant attaque est bonne (le nombre d'erreurs est de 1/32 bits). Cependant, le deuxième schéma, qui représente le comportement du détecteur après une compression JPEG à 70% de qualité, montre une moins bonne détection pour cet exemple : le nombre d'erreurs obtenu est de 4/32 bits, ce qui constitue un résultat médiocre pour une telle valeur de la redondance.

Conclusion

La méthode de tatouage par paquet d'ondelettes à laquelle nous rajoutons l'étape de correction de l'image permet de contrôler exactement la qualité du marquage. Cependant, comme l'opération de correction des modifications est externe au processus de marquage,

FIG. 11.1 – Image originale et masque psychovisuel

FIG. 11.2 – Image originale et masque psychovisuel

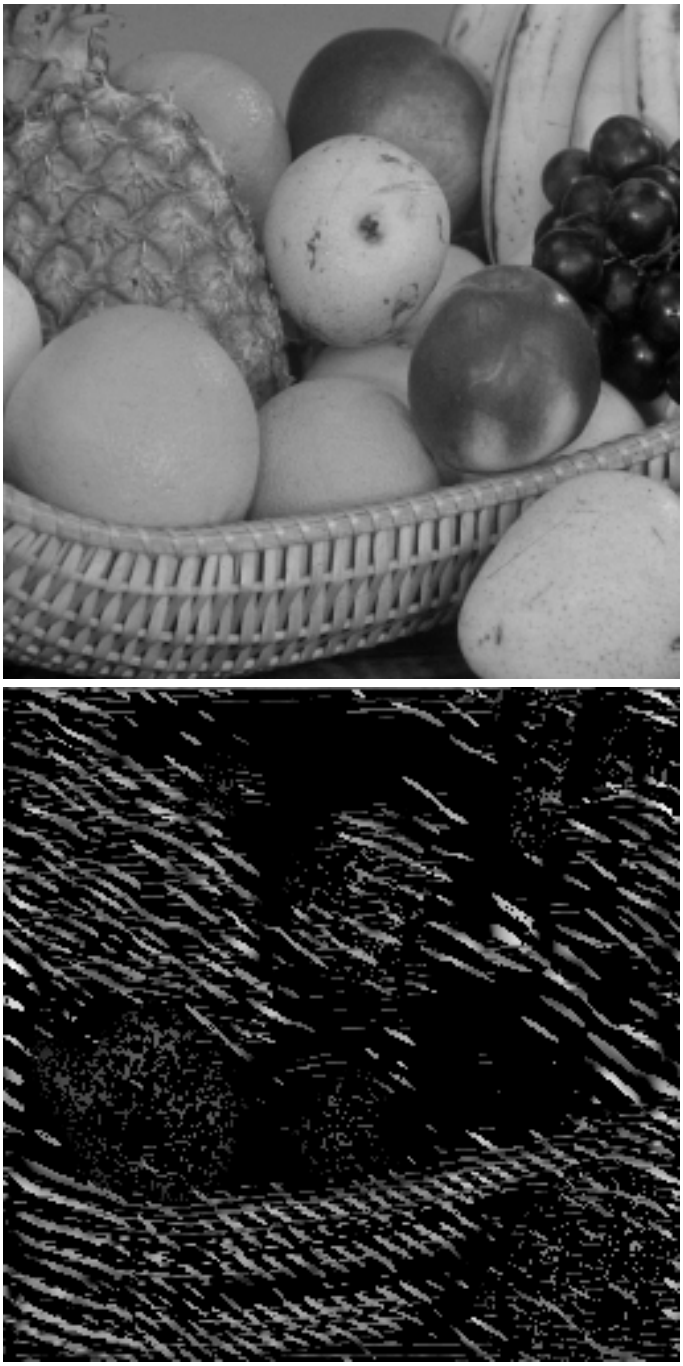


FIG. 11.3 – Image originale et masque psychovisuel

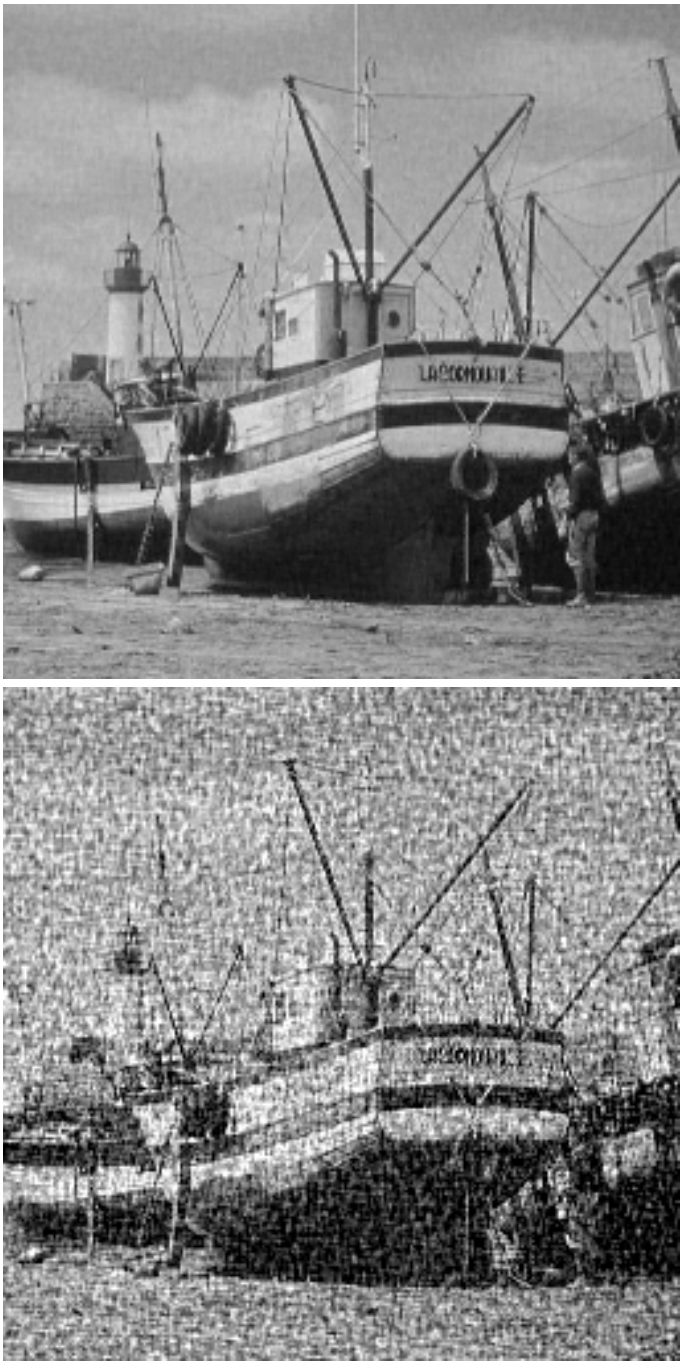


FIG. 11.4 – Image fortement tatouée et image sur laquelle les distorsions sont amplifiées d'un facteur de 10.

FIG. 11.5 – Image résultat de la correction par le masque psychovisuel.

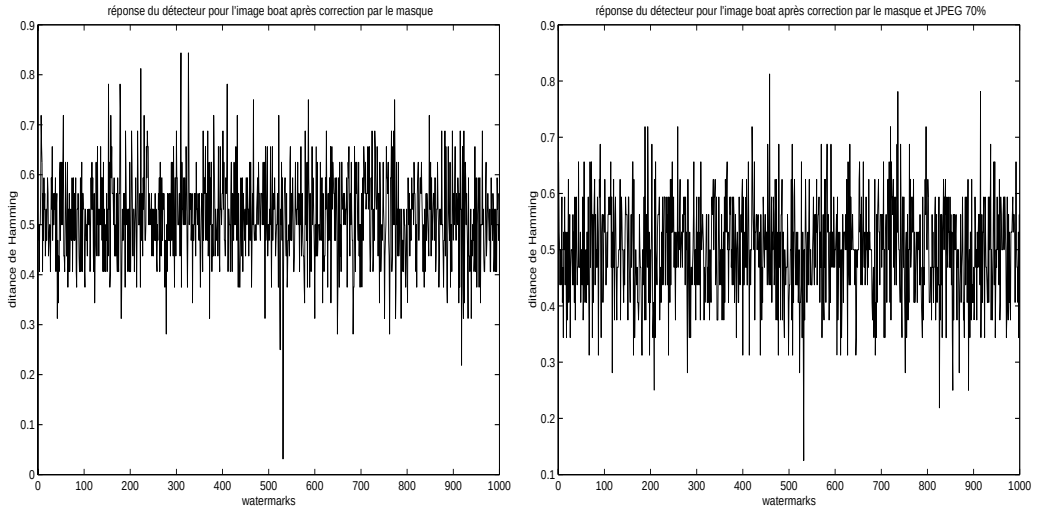


FIG. 11.6 – Réponse du détecteur pour 1000 watermarques générées aléatoirement après correction de l'image tatouée, sans attaque puis après une compression JPEG à 70% de qualité

elle apparaît comme une attaque et on ne contrôle plus ici la robustesse du tatouage. Nous avons donc décidé de ne pas étudier plus avant cette méthode. Nous allons présenter dans le paragraphe suivant une autre solution permettant d'utiliser les outils psychovisuels et qui ne présente pas cet inconvénient.

11.3 Optimisation par critère psychovisuel des paramètres de modifications

Nous avons vu au paragraphe 7 que l'étape génératrice d'artefacts visibles est celle où l'on implante le code, c'est-à-dire l'étape où l'on modifie les coefficients pointés par la sous base et par la watermarque (voir le paragraphe 6.2.3.6). Dans ce paragraphe, notre objectif est d'optimiser le coefficient ε de force du tatouage en fonction du critère psychovisuel présenté au paragraphe 11.1. L'équation présentée ci-dessous rappelle le principe de la modification d'un noeud i (où i est le multi-indice représentant la profondeur et la bande de fréquence considérée) :

$$C_i^*(k) = \alpha_i C_i(k) \tag{11.2}$$

avec

$$\alpha_i = \sqrt{\frac{s+\varepsilon}{\|C_i^*\|_2^2}} \tag{11.3}$$

11.3.1 Principe de l'optimisation

Le masque psychovisuel n'a de signification que dans le domaine spatial. La première partie du travail présenté ici consistera donc à exprimer les modifications que l'on fait sur les coefficients en paquets d'ondelettes dans le domaine spatial.

11.3.1.1 Expression des modifications de l'image dans le domaine spatial

L'équation de reconstruction d'une image I décomposée sur une base de paquets d'ondelettes B est présentée ci-dessous :

$$I(i,j) = \sum_{(p,k,l)\in B} \sum_{m,n} C_{p,k,l}(m,n) W_{p,k,l,m,n}(i,j) \tag{11.4}$$

Les ondelettes W sont les ondelettes séparables définies au paragraphe 4.3 et respectant l'équation suivante :

$$W_{p,k,l,m,n}(i,j) = \frac{1}{2^{-p}} W_k(2^{-p}i - m) W_l(2^{-p}j - n) \tag{11.5}$$

Dans ces deux équations, le couple (i,j) représente les pixels de l'image, les paramètres m et n représentent les translations spatiales. p est le niveau de résolution du paquet traité. k et l sont les indices des bandes fréquentielles du paquet. B représente une base.

Pour simplifier les notations, nous utiliserons le multi-indice k décrivant à la fois le niveau de résolution et la bande de fréquence du paquet. L'équation de reconstruction devient alors :

$$I(i,j) = \sum_{k \in B} \sum_{m,n} C_k(m,n) W_{k,m,n}(i,j) \tag{11.6}$$

On fait la décomposition de l'image I sur la base B^* représentant la meilleure base obtenue après tatouage de l'image. On note $B^* = SB^*_{mod} \bigcup SB^*_{nonmod}$, c'est à dire que l'on sépare les noeuds des coefficients modifiés et non modifiés dans B^*. L'équation de reconstruction devient alors, pour toute image I :

$$I(i,j) = \sum_{k \in SB^*_{mod}} \sum_{m,n} C_k(m,n) W_{k,m,n}(i,j) + \sum_{k \in SB^*_{nonmod}} \sum_{m,n} C_k(m,n) W_{k,m,n}(i,j) \tag{11.7}$$

On exprime la différence des images originale et tatouée sur cette base. Seuls les paquets de SB^*_{mod} ne sont pas nuls (on néglige les modifications apportées par l'étape de stabilisation).

$$I^*(i,j) - I(i,j) = \sum_{k \in SB^*_{mod}} \sum_{m,n} (C^*_k(m,n) - C_k(m,n)) W_{k,m,n}(i,j) \tag{11.8}$$

ainsi, en utilisant la formule 11.2 on obtient :

$$I^*(i,j) - I(i,j) = \sum_{k \in SB^*_{mod}} (\alpha_k - 1) \sum_{m,n} C_k(m,n) W_{k,m,n}(i,j) \tag{11.9}$$

La deuxième somme de l'équation représente l'image obtenue par inversion de la décomposition en bases de paquets d'ondelettes de l'unique paquet k, toutes les contributions relatives aux autres paquets ayant été annulées. Appelons I_k l'image obtenue par reconstruction du seul paquet k ($I_k(i,j) = \sum_{m,n} C_k(m,n) W_{k,m,n}(i,j)$). La relation 11.9 devient :

$$I^*(i,j) - I(i,j) = \sum_{k \in SB^*_{mod}} (\alpha_k - 1) I_k(i,j) \tag{11.10}$$

Cette équation signifie que les modifications se font en augmentant les gains d'un ensemble d'images issues du filtrage de l'image hôte par un banc de filtres. Ces filtres sont caractérisés par l'ondelette choisie et par les paquets concernés. Cette équation nous donne l'expression des modifications de l'image dans le domaine spatial, nous allons donc pouvoir appliquer le modèle psychovisuel.

11.3.1.2 Contrainte psychovisuelle

Le tatouage ne sera pas perceptible au sens de notre critère si l'image modifiée I^* respecte la relation 11.1 c'est-à-dire si pour tout pixel (i,j) de l'image, on a :

$$|(I(i,j) - I^*(i,j))| \leq F(i,j) \tag{11.11}$$

Cette relation implique la condition suivante sur les paramètres α_k :

$$\forall(i,j), |\sum_{k \in SB^*_{mod}} (\alpha_k - 1) I_k(i,j)| \leq F(i,j) \tag{11.12}$$

La relation 11.12 nous donne le système d'inéquations que doivent respecter les coefficients α_k afin que les modifications soient imperceptibles. Nous pouvons rajouter à celles-ci les conditions suivantes : afin que l'image I^* soit effectivement tatouée, il faut imposer que les coefficients α_k soient supérieurs à 1. De plus, la robustesse maximale sera obtenue pour α_k maximum.

Nous rechercherons donc à maximiser la valeur de chaque coefficient $\{\alpha_k\}$ avec $\alpha_k > 1$ telle que la relation 11.12 soit respectée pour tous les pixels de l'image.

11.3.2 Résultats

Afin de résoudre l'optimisation en tenant compte des contraintes décrites par le système d'inéquations 11.12, il faut inverser la décomposition en paquets d'ondelettes pour chaque noeud modifié. Appelons N_m le nombre de noeuds modifiés et $N \times N$ la taille de l'image. Notre objectif est de maximiser la valeur de N_m coefficients soumis à $N * N$ contraintes. Des raisons calculatoires, nous ont poussé à diminuer considérablement la taille de la marque (la redondance maximale est de 2 pour une marque de 32 bits). Nous arrêterons de plus la décomposition de l'arbre à un niveau $p = 5$ (au lieu de 8). Ainsi, le nombre N_m de modifications est fortement diminué. De plus, il arrive que le système d'inéquation 11.12 n'ait pas toujours de solution telle que $\alpha_k > 1$, nous avons rajouté alors au masque une matrice constante de quelques bits.

Nous avons implanté une marque de 32×2 bits sur l'image Lenna. Nous présentons ici les résultats obtenus pour un tatouage dont les forces ne sont pas contraintes (nous l'appellerons T_f), et pour un tatouage dont les forces correspondent à la méthode présentée dans ce paragraphe (T_o).

La figure 11.7 présente l'image tatouée résultat de T_f, la force du tatouage est fixée à $\varepsilon = 3s$. Les modifications sont visibles sur support numérique et le PSNR est de $23,8$ dB. La figure 11.8 présente la différence entre l'image tatouée et l'originale, amplifiée d'un facteur multiplicatif de $15,7$.

L'image 11.9 présente la même image marquée avec la même watermarque et avec la même clef sur laquelle nous avons appliquée le processus T_o. L'image obtenue est de bonne qualité, le PSNR est de $38,37$ dB. La figure 11.10 présente l'image différence obtenue avec le même coefficient d'amplification de $15,7$. L'amplitude des différences a considérablement baissée. On vérifie que les modifications sont présentes aux endroits autorisés par le masque (voir la figure 11.2). En ce qui concerne l'imperceptibilité de la marque, la méthode donne de bons résultats sur cet exemple.

FIG. 11.7 – Image tatouée avec une grande force de tatouage

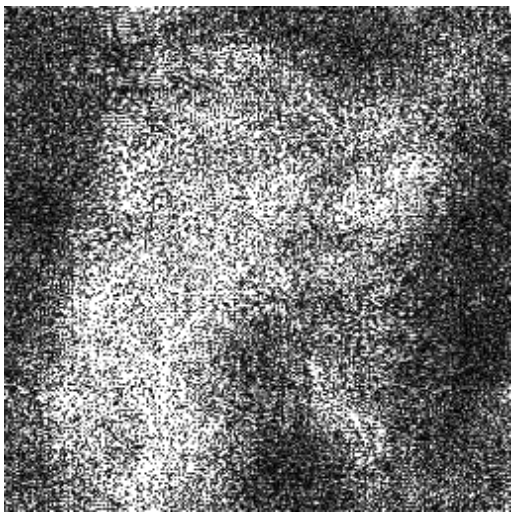


FIG. 11.8 – Image différence des images fortement tatouée et originale, les niveaux de gris ont été amplifiés d'un facteur de 15.7

FIG. 11.9 – Image tatouée avec des coefficients de force de tatouage optimisés

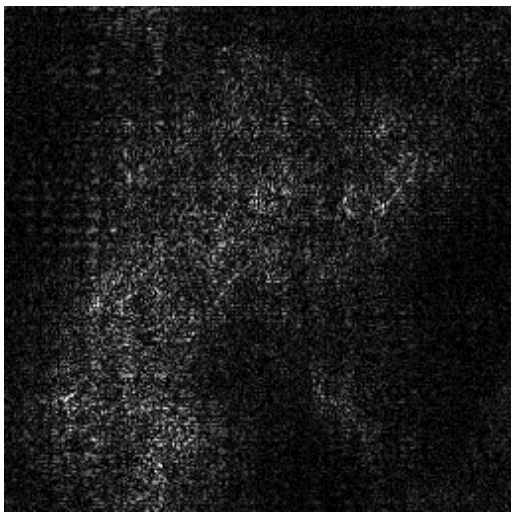


FIG. 11.10 – Différence entre l'image tatouée avec optimisation des forces et l'image originale, les niveaux de gris ont été amplifiés d'un facteur de 15.7

Nous allons maintenant comparer la robustesse des deux méthodes. Dans le cas T_f, la robustesse est bonne (le coefficient d'erreur est inférieur à 2 bits sur 32) pour une compression JPEG de coefficient de qualité variant de 100% à 65% de qualité. Dans le cas T_o, les résultats sont moins bons : la détection sans attaque présente un coefficient d'erreur de 2/32 (voir figure 11.11) et après une attaque, cette détection présente un coefficient d'erreur de 4/32, ce qui est un résultat médiocre (voir la figure 11.12) du à la diminution de la valeur des coefficients de force du tatouage.

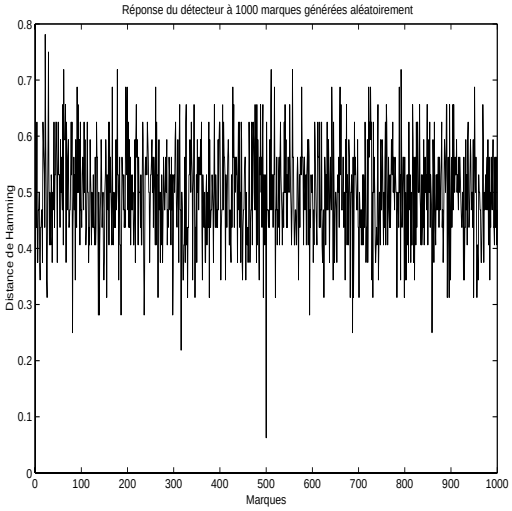


FIG. 11.11 – Réponse du détecteur pour 1000 watermarques générées aléatoirement après optimisation des coefficients de force sans attaque

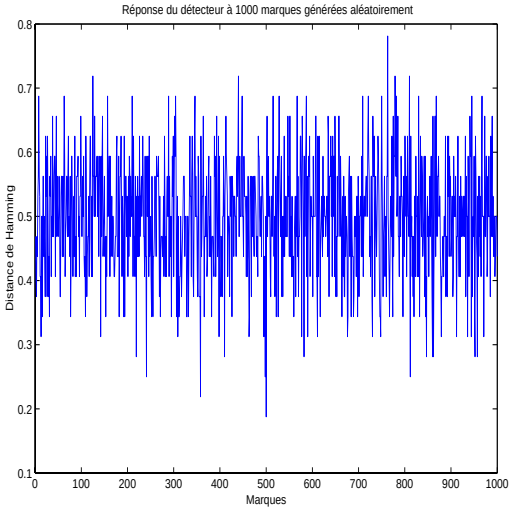


FIG. 11.12 – Réponse du détecteur pour 1000 watermarques générées aléatoirement après optimisation des coefficients de force et compression JPEG de 70% de qualité

11.4 Conclusion

Nous avons présenté dans cette partie deux méthodes permettant de contrôler la qualité perceptuelle du tatouage d'une image. La première consiste à corriger l'image obtenue après tatouage à l'aide d'un masque psychovisuel. Cette méthode donne évidemment de bons résultats en ce qui concerne l'imperceptibilité de la marque. Cependant, l'étape de correction de l'image étant externe à l'algorithme de tatouage, on ne peut plus contrôler le tatouage, c'est-à-dire que l'on ne peut pas assurer que la marque reste présente après cette correction. Cette méthode n'étant pas considérée comme fiable, nous avons développé une autre méthode qui n'a pas cet inconvénient.

La seconde méthode proposée dans ce chapitre consiste à optimiser les modifications que l'image hôte subit dès l'étape d'implémentation de la marque. Cela revient à optimiser les coefficients de force du tatouage. La principale difficulté de cette optimisation consiste à exprimer les modifications des coefficients de paquets d'ondelettes dans le domaine spatial. En effet, le masque psychovisuel n'a de sens que dans ce domaine. Cette contrainte est réalisable en inversant la décomposition en paquets d'ondelettes. L'optimisation des coefficients de forces se fait alors sur un ensemble d'images issues de l'image hôte par filtrage par un banc de filtres. La réalisation pratique de cette optimisation demandant beaucoup de temps de calculs, cette méthode n'est valable que pour l'insertion d'une petite clef. En ce qui concerne l'invisibilité, les résultats sont très satisfaisants. Les contraintes d'invisibilité diminuant la valeur de certains coefficients de force du tatouage, il est évident que les performances de robustesse s'en trouvent dégradées.

Les deux méthodes obtenues dans ce chapitre ne permettent pas d'améliorer les performances de la méthode de tatouage par paquets d'ondelettes. En effet, si on les utilise, le tatouage est alors imperceptible mais dans le premier cas, on ne peut pas assurer que la marque reste présente. Dans le second cas, les contraintes apportées par l'utilisation du masque nous obligent à réduire la longueur de la marque. De plus, les performances du détecteurs sont alors dégradées. Une solution pour pallier à ces problèmes serait d'utiliser des critères psychovisuels calculés directement dans le domaine des paquets d'ondelettes. On pourrait aussi utiliser la décomposition en canaux perceptuels décrite dans le paragraphe 2.1.2 : en calquant cette décomposition sur la décomposition en paquets d'ondelettes, on obtiendrait alors un ensemble de paquets susceptibles d'être modifiés sans créer d'artefacts visibles.

Chapitre 12

Choix de la watermarque

Nous avons vus lors des chapitres précédents qu'afin d'obtenir de meilleures performances à la détection, nous utilisons de la redondance lors de l'implantation du message. Or, d'autres techniques de correction de codes existent et sont plus performantes pour corriger d'éventuelles erreurs que la redondance. Notre objectif dans ce chapitre est de présenter l'une d'elles et d'étudier les avantages que son utilisation apporte à notre méthode de tatouage. Notre choix c'est porté sur l'utilisation de m-séquences, très populaire dans les méthodes de tatouages additives. La première partie de ce chapitre présente ces séquences de façon théorique. Nous nous appuierons sur les études présentées par C. Fontaine [58] et R.J. McEliece [59]. Dans la seconde partie nous nous intéresserons à l'utilisation de ces séquences dans le cas du tatouage par extraction. Nous étudierons les probabilité de fausses alarmes et les probabilités de manques à la détection que l'utilisation des m-séquences engendre. Nous conclurons ce chapitre en comparant la méthode de détection utilisant les m-séquences avec la méthode classique de détection utilisant la redondance du message et la distance de Hamming.

12.1 Définition et création de m-Séquences

Une m-séquence est une suite binaire pseudo-aléatoire (générée de façon déterministe) possédant des propriétés mathématiques (en particulier de corrélation) qui en font un outil très présent dans les techniques de codage et de télécommunication. Pour présenter cet outil, nous allons directement expliquer comment la générer.

12.1.1 Génération d'une m-Séquence

12.1.1.1 Exemple

Une m-séquence est une suite de valeurs binaires. Elle est caractérisée par ses premières valeurs et une relation de redondance. Cette relation peut être exprimée à l'aide d'un registre. Afin de simplifier le propos, nous allons présenter dès maintenant un exemple de registre et expliquer la création de la m-séquence.

La figure 12.1 présente un registre de longueur L. A chaque top d'horloge, s_i (le bit de poids faible du registre) constitue la sortie, tous les bits sont décalés vers la droite ; s_{i+L}, placé dans le bit de poids fort est donné par l'équation linéaire :

$$s_{i+L} = c_1.s_{i+L-1} + c_2.s_{i+L-2} + ... + c_{L-1}.s_{i+1} + c_L.s_i$$

L'entrée du registre est donnée par une équation linéaire portant sur les éléments du registre, on dit que le registre est à rétroaction linéaire. La suite formée par les sorties du registre est la M-séquence.

FIG. 12.1 – Registre à décalage à rétroaction linéaire de longueur L

12.1.1.2 Définitions

L'exemple présenté ci-dessus donne le schéma général de la création d'une M-séquence. Nous allons compléter ce schéma par les définitions rigoureuses permettant de caractériser une M-séquence.

Définition du registre

Définition 6 *Un registre à décalage à rétroaction linéaire (LFSR) binaire de longueur L est un registre à décalage contenant une suite L de bits* $(s_i, s_{i+1}, ...s_{i+L-1})$ *et une fonction de rétroaction linéaire.*

Définition 7 *Les bits* $(s_0, ..., s_{L-1})$ *qui déterminent entièrement la suite produite constituent l'état initial du registre.*

Définition de la relation de redondance définissant la M-séquence Dans ce paragraphe nous noterons $F_2[X]$ l'ensemble des polynômes de coefficients appartenant à $\{0, 1\}$, $GF[2]$ sera l'anneau associé.

Définition 8 *Le polynôme de rétroaction est le polynôme de* $F_2[X]$ *:*

$$f(X) = 1 + c_1X + c_2X^2 + ... + c_LX^L$$

Définition 9 *Le polynôme de rétroaction minimal de la suite est le diviseur de* $f(X)$ *de plus bas degré parmi les polynômes de tous les LFSR possibles générant* $(s_n)_{n\geq 0}$

Définition 10 *L'ordre de $P(X)$ où $P(0) \neq 0$ est le plus petit entier e, tel que $P(X)$ divise $x^e + 1$.*

Exemple : Dans $GF[2]$ $P(X) = X^5 + X^2 + 1$ est de degré 31 car $\frac{X^{31}+1}{X^5+X^2+1} = Q(X)$ où Q est un polynôme.

Proposition 1 *Les polynômes de l'ensemble fini $GF[2]$ sont primitifs si ils sont d'ordre $2^n - 1$ où n est le degré du polynôme.*

M-séquences

Définition 11 *Si le polynôme de rétroaction minimal du LFSR est primitif et que son état initial est non nul. Alors la suite produite est de période maximale $2^L - 1$ et est dite suite ML.*

Le nombre de polynômes primitifs sur $GF[2]$ pour $n = 1, 2, ...$ est $1, 1, 2, 2, 18, 16, 48, ...$ Une M-séquence de longueur 31 est générée par un registre de longueur 5.

12.1.2 Propriétés des m-Séquences

Les m-séquences ont plusieurs propriétés remarquables, nous nous intéresserons ici plus particulièrement aux propriétés de sa fonction d'autocorrélation.

Pour une séquence x donnée, sa fonction d'autocorrélation $C(\tau)$ est définie comme la corrélation entre x et sa version cycliquement décalée τ fois. Pour des raisons calculatoires, nous prenons les valeurs des composantes de x dans $\{-1, 1\}$ plutôt que dans $\{0, 1\}$. Avec cette convention, $C(x, y) = \sum x_i y_i$ et la fonction d'autocorrélation est :

$$C(\tau) = \sum_{i=0}^{n-1} x_i x_{i+\tau}$$

Théoreme 2 *Si $(s_i)_{i=0}^{n-1}$ est une m-séquence de longueur $n = 2^L - 1$, alors*

$$\begin{aligned} C(\tau) &= -1 \quad si\ \tau \neq 0 \pmod n \\ &= n \quad si\ \tau = 0 \pmod n. \end{aligned}$$

Les propriétés de corrélations particulières d'une m-séquence peuvent avoir un impact bénéfique sur les performances du détecteur de système de tatouage. Nous allons maintenant étudier cette application particulière et en particulier lorsque l'on travaille dans un environnement bruité.

12.2 Application au tatouage dans le cas de la détection par vérification

Nous nous intéressons ici au cas de vérification d'un tatouage extrait, ce qui constitue l'étape finale de notre processus de détection. l'objectif est de déterminer si la marque

extraite correspond bien à celle implantée. Si la marque est une m-séquence, il suffit de vérifier que la marque extraite possède une fonction d'autocorrélation idéale avec sa version originale supposée.

Dans le paragraphe suivant, nous allons définir et optimiser le choix d'un paramètre de décision d. La comparaison entre ce seuil et la valeur de corrélation nous permettra de dire si la marque extraite est celle voulue et cela même si il y a des erreurs d'extraction.

12.2.0.1 Procédure de décision

Classiquement, nous définissons deux classes de décision :
- w_1 est la classe de la m-séquence originale s et de ses versions dégradées
- w_2 la classe des signaux restant (ils sont binaires dans $\{-1,1\}^n$)

Soient alors deux hypothèses
- H_1 : $\hat{s}$ appartient à w_1
- H_2 : $\hat{s}$ appartient à w_2

Le test de décision est basé sur les propriétés de corrélations des m-Séquences, pour un seuil d :
- On décide H_1 si : $\hat{C(0)} > d$ et si $\forall k \in [1, n-1], \hat{C(k)} < d$
- On décide H_2 sinon

Avec

$$\hat{C(\tau)} = \sum_{k=0}^{n-1} \hat{s_k} s_{k+\tau}$$

Le but est de réduire les probabilités d'erreurs de première et de deuxième espèces avec
- P_{e1} probabilité d'erreur de première espèce, c'est la probabilité de choisir H_2 sachant w_1 ou probabilité de faux négatif
- P_{e2} probabilité d'erreur de deuxième espèce, c'est la probabilité de choisir H_1 sachant w_2 ou probabilité de faux positif

Soit c_1 fonction de corrélation d'une suite de w_1, c_2 d'une suite de w_2, on a alors les relations suivantes :
- $P_{e1} = P(c_1(0) < d \quad ou \quad c_1(k) > d)$
- $P_{e2} = P(c_2(0) > d \quad et \quad \forall k \in [1, n-1], c_2(k) < d)$

où P désigne la probabilité.

Les probabilités d'erreurs de première et deuxième espèces se caractérisent donc par :

$$P_{e1} = P(c_1(0) < d) + \frac{1}{n-1} \sum_{k=1}^{n-1} P(c_1(k) > d) \tag{12.1}$$

$$P_{e2} = P(c_2(0) > d) \prod_{k=1}^{n-1} P(c_2(k) < d) \tag{12.2}$$

La figure 12.2 montre les variations des fonctions de corrélation suivant les décalages et pour plusieurs signaux. Le premier graphique montre une corrélation parfaite pour

une m-séquence non dégradée. Dans le second, un bruit blanc est utilisé comme signal, la corrélation n'est pas parfaite, la détection sera meilleure dans le premier cas. Les trois graphiques suivants sont réalisés pour une m-Séquence dégradée de respectivement 4, 8 et 12 bits pour une longueur de 31 bits. Pour ces deux premiers exemples, la détection est encore possible, pour le dernier, le pic caractéristique en zéro a disparu, on ne pourra pas détecter la marque. Dans ces exemples, le seuil d de détection est matérialisé par la droite horizontale à $d = 10$, la suite de cette étude aura pour but de préciser la valeur de ce seuil. Dans le paragraphe suivant, nous caractériserons les deux classes de signal.

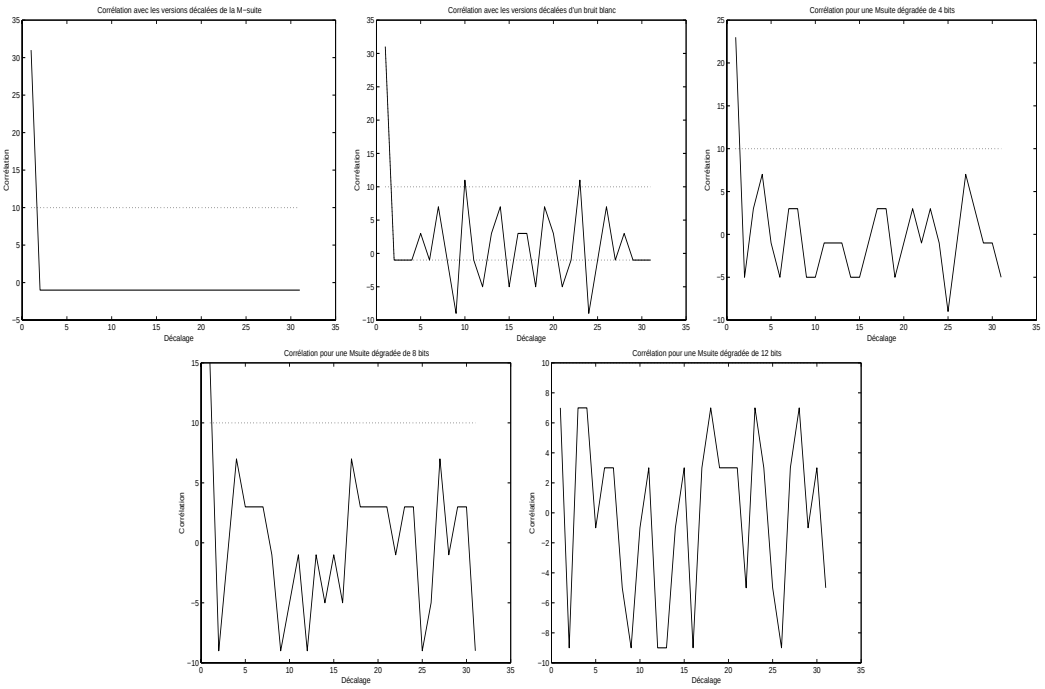


FIG. 12.2 – Corrélations entre un signal et ses versions décalées pour une m-séquence, un bruit blanc et des m-séquences dégradées

12.2.1 Caractérisation des deux classes de signaux

12.2.1.1 Caractérisation de la classe w_1

Une particularité de cette étude tient en la définition de w_1, nous allons ici mieux caractériser cette classe de signaux et étudier plus précisément les propriétés des corrélations.

Proposition 3 *Une suite $\hat{s}$ de $\{-1, 1\}^n$ est une version dégradée de s si et seulement si*

$$\exists k \in [0, n-1] \quad / \quad \hat{s_k} = -s_k \tag{12.3}$$

Corrélation Soit D, l'ensemble des bits dégradés de $\hat{s}$: $D = \{k \in [0, n-1] \quad / \quad \hat{s_k} = -s_k = s_k - 2s_k\}$ et soit ND son complémentaire dans $[0, n-1]$, notons $\hat{C}(\tau)$ la corrélation obtenue entre une version dégradée $\hat{s}$ de la suite s, et les versions décalées de s, on obtient :

$$\begin{aligned}
\hat{C}(\tau) &= \sum_{ND} \hat{s_k} s_{k+\tau} + \sum_{D} \hat{s_k} s_{k+\tau} \\
\hat{C}(\tau) &= \sum_{ND} s_k s_{k+\tau} + \sum_{D} (s_k - 2s_k) s_{k+\tau} \\
\hat{C}(\tau) &= \sum_{ND+D} s_k s_{k+\tau} - 2 \sum_{D} s_k s_{k+\tau}
\end{aligned} \tag{12.4}$$

Appelons v_i le **vecteur** contenant les indices des bits dégradés de $\hat{s_k}$, i étant la longueur de v, *i.e.* le nombre de dégradations. On obtient :

$$\hat{C}(\tau) = C(\tau) - 2S(\tau, v_i) \tag{12.5}$$

avec $S(\tau, v_i) = \sum_{v_i} s_k s_{k+\tau}$. On a $S(\tau, v_n) = C(\tau)$. On impose $S(\tau, v_0) = 0$ (il n'y a aucune dégradation).
De plus, $\forall i \in [0, n], \quad S(0, v_i) = i$, d'où

$$\hat{C(0)} = n - 2i \tag{12.6}$$

Dans les deux paragraphes suivants, nous étudierons la suite S. Nous trouverons des relations statistiques permettant de calculer les probabilités d'erreurs.

12.2.1.2 Statistiques de S

L'idée principale de l'étude que nous développons ici est d'exprimer le produit $s_k s_{k+\tau}$ sous forme d'une variable aléatoire réalisation x_k de X.

Les corrélations de la m-séquence dégradée avec les versions décalées de la m-séquence d'origine respectent les formules suivantes

$$\begin{aligned}
\forall \tau \neq 0 \pmod n, \quad & E(\hat{C(\tau)}) = E(C(\tau)) - 2E(S(\tau, v_i)) = -1 - 2E(S(\tau, v_i)) \\
& \sigma^2(\hat{C(\tau)}) = \sigma^2(C(\tau)) + 4\sigma^2(S(\tau, v_i)) = 4\sigma^2(S(\tau, v_i))
\end{aligned} \tag{12.7}$$

où E est l'espérance mathématique et σ l'écart type. C est déterministe.

Les seules connaissances que nous ayons sur la suite x_k est que $\forall k, \ x_k \in \{-1, 1\}$ et de plus, $\{x_k\}$ respecte la relation suivante

$$\sum_{k=0}^{n-1} x_k = -1 \tag{12.8}$$

Nous allons modéliser la suite de variables x_k par une suite de variables identiquement distribuées respectant la relation 12.8 au premier et deuxième ordre. Les x_k sont alors des variables de Bernoulli appartenant à $\{-1, 1\}$ qui respectent les relations suivantes :

$$E(\sum_{k=0}^{n-1} x_k) = -1 \tag{12.9}$$

ce qui signifie :

$$E(x_k) = \frac{-1}{n} \tag{12.10}$$

On peut aussi calculer la variance de x_k :

$$\begin{aligned} \sigma^2(X) &= E(X^2) - E(X)^2 \\ \sigma^2(X) &= 1 - \frac{1}{n^2} \end{aligned} \tag{12.11}$$

L'équation 12.8 prise au deuxième ordre implique les relations suivantes :

$$\begin{aligned} E((\sum_{k=0}^{n-1} x_k)^2) &= 1 \\ \sum_{k=0}^{n-1} E((x_k)^2) + \sum_{k \neq j} E(x_k x_j) &= 1 \\ n + n(n-1)E(x_k x_j) &= 1 \end{aligned} \tag{12.12}$$

ce qui implique

$$\forall k \neq j,\ E(x_k x_j) = \frac{-1}{n} \tag{12.13}$$

Soit alors $Z_i = \sum_{v_i} x_k$ ($Z_i = S(\tau, v_i)$). On obtient tout naturellement l'espérance de cette somme par

$$E(Z_i) = \frac{-i}{n} \tag{12.14}$$

La variance s'exprime de la façon suivante

$$\begin{aligned} \sigma^2(Z_i) &= E(Z_i^2) - E(Z_i)^2 \\ \sigma^2(Z_i) &= E((\sum_{k=0}^{i-1} x_k)^2) - \frac{i^2}{n^2} \\ \sigma^2(Z_i) &= i + i(i-1)E(x_k x_i) - \frac{i^2}{n^2} \\ \sigma^2(Z_i) &= i + i(i-1)(\frac{-1}{n}) - \frac{i^2}{n^2} \end{aligned} \tag{12.15}$$

La variance de Z est alors

$$\sigma^2(Z_i) = (1 + \frac{1}{n})i(1 - \frac{i}{n}) \tag{12.16}$$

Un élément de la classe 1, dont i bits ont été dégradés a donc une corrélation $\hat{C}$ de la forme

$$\hat{C}(0) = n - 2i \tag{12.17}$$

$$\forall \tau \neq 0 \pmod{n}, \quad E(\hat{C}(\tau)) = -1 + 2\frac{i}{n} \qquad \sigma^2(\hat{C}(\tau)) = 4i(1+\frac{1}{n})(1-\frac{i}{n}) \tag{12.18}$$

La figure 12.3 présente l'évolution de l'espérance de $\hat{C(\tau)}$ pour tout $\tau \neq 0$ modulo n selon les dégradations v_i où i est représenté en abscisses. La droite en pointillés présente la valeur théorique, l'autre courbe présente les résultats obtenus pour une m-séquence de longueur 31 dégradée. Pour chaque valeurs de i, le vecteur v_i est calculé aléatoirement. La figure 12.4 présente le même résultat pour 3 m-séquences dégradées. Nous avons présenté ces mêmes résultats pour la variance de la fonction de corrélation sur les figures 12.5 et 12.6. Les courbes théoriques suivent bien les courbes obtenues par simulation.

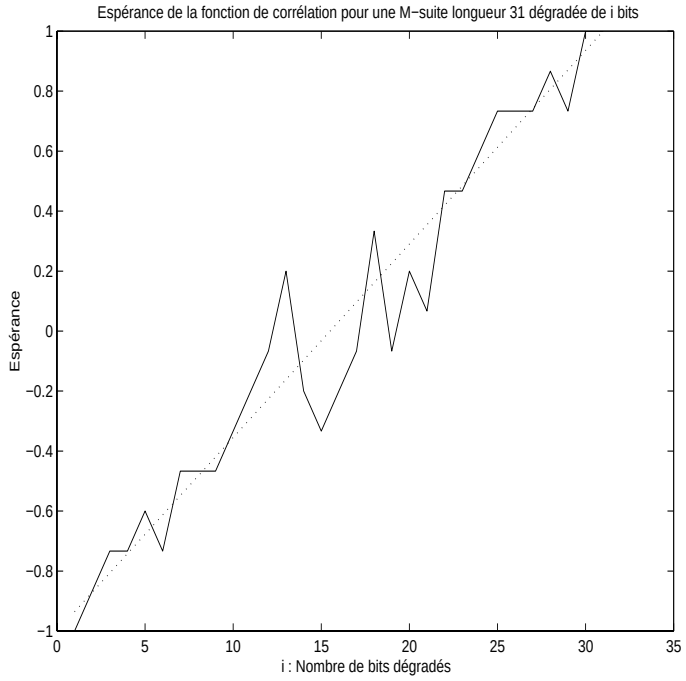


FIG. 12.3 – Espérance de $\hat{C}(\tau)$ selon les dégradations de la m-séquence. Courbe théorique (pointillés) et courbe réelle obtenue par simulation sur une m-séquence de longueur 31.

La figure 12.7 présente les valeurs de la fonction d'autocorrélation pour tous les décalages τ et selon le nombre de dégradations i pour 100 réalisations de v_i. La droite avec des «plus» correspond aux valeurs de $\hat{C(0)}$. Les points correspondent aux valeurs obtenues pour les autres décalages. La figure 12.8 représente cette même courbe sur laquelle nous avons rajouté les domaines de confiance à 95% et à 99% (pointillés) que nous avons calculés grâce à l'étude statistique faite dans ce paragraphe.

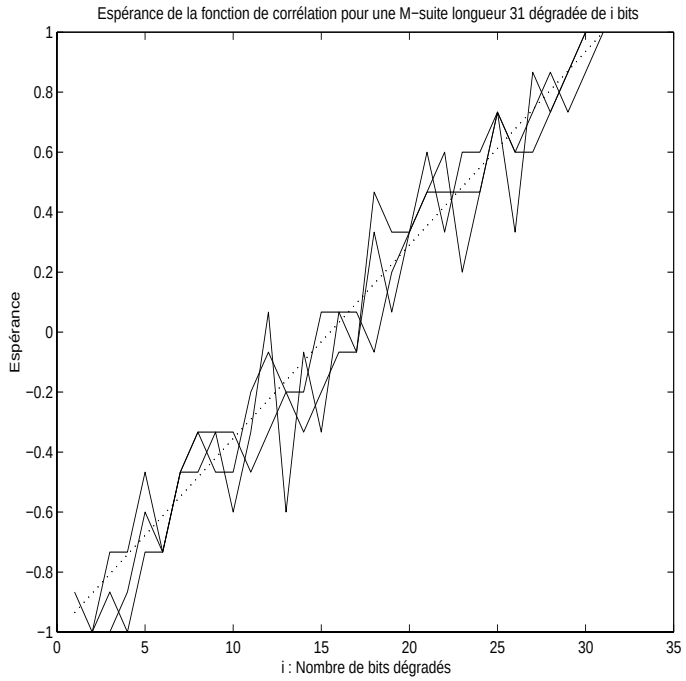


FIG. 12.4 – Espérance de $\hat{C}(\tau)$ selon les dégradations de la m-séquence. Courbe théorique (pointillés) et courbe réelle obtenue par simulation sur trois m-séquences de longueur 31.

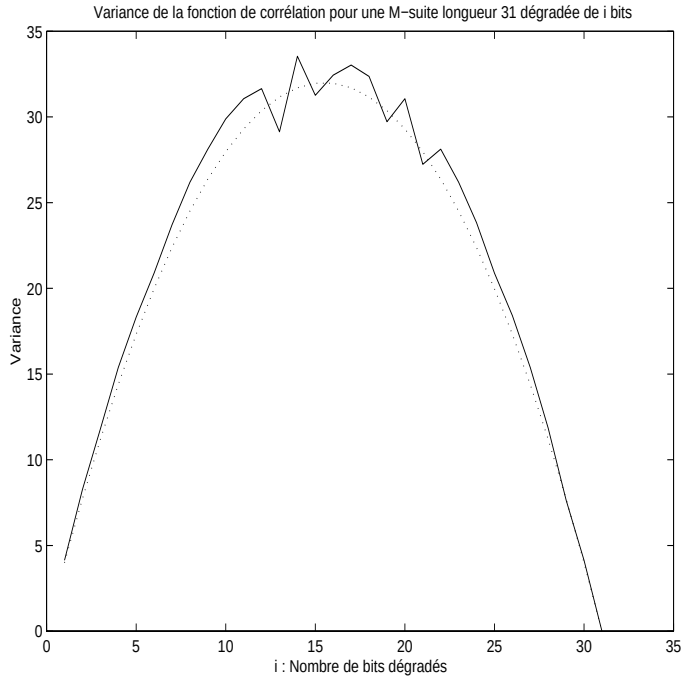


FIG. 12.5 – Variance de $\hat{C}(\tau)$ selon les dégradations de la m-séquence. Courbe théorique (pointillés) et courbe réelle obtenue par simulation sur une m-séquence de longueur 31.

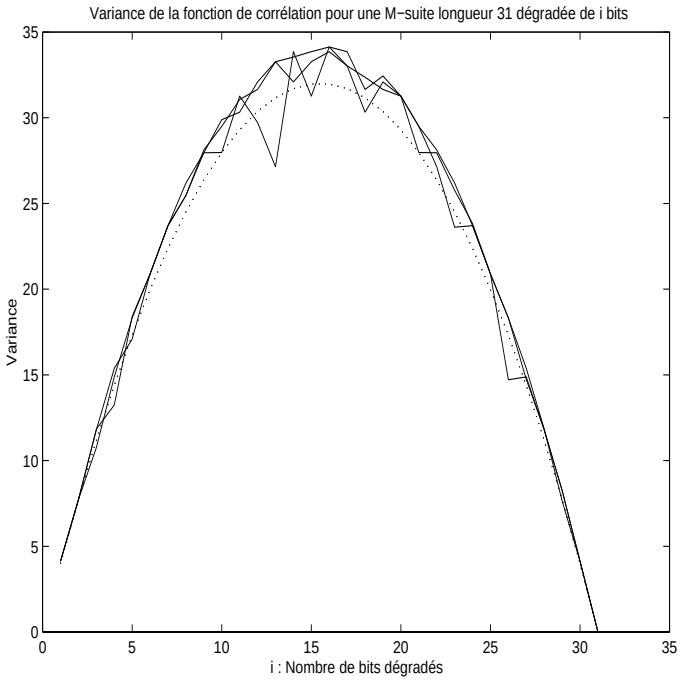


FIG. 12.6 – Variance de $\hat{C}(\tau)$ selon les dégradations de la m-séquence. Courbe théorique (pointillés) et courbe réelle obtenue par simulation sur une m-séquence de longueur 31.

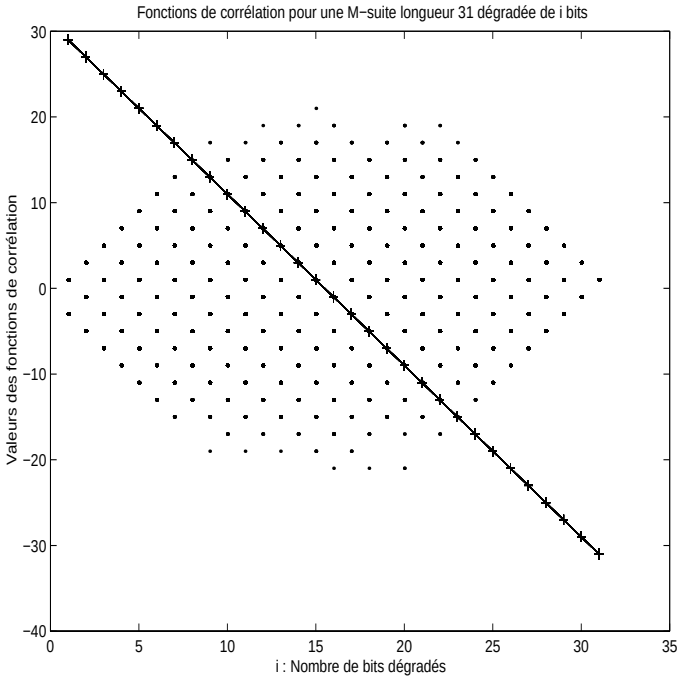


FIG. 12.7 – Répartition des valeurs de $\hat{C}(\tau)$ selon les dégradations i. Les «+» représentent les valeurs obtenus pour $\hat{C}(0)$.

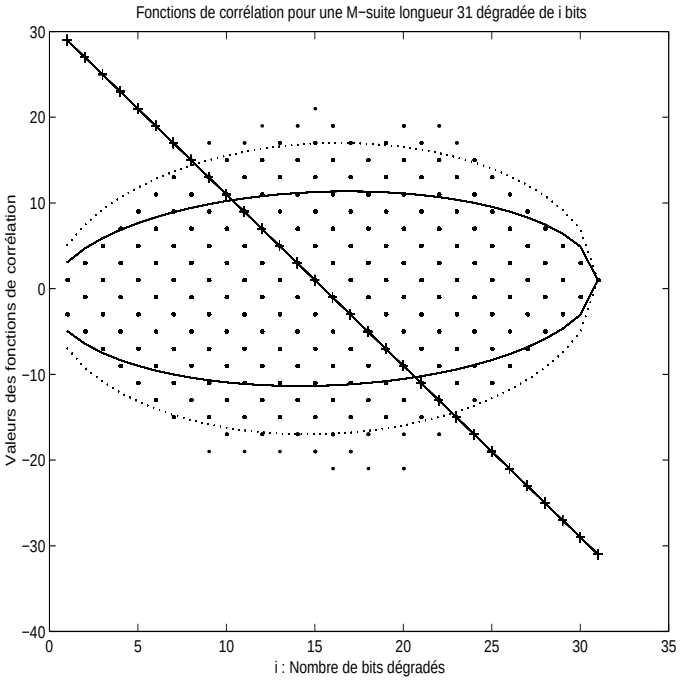


FIG. 12.8 – Répartition des valeurs de $\hat{C}(\tau)$ selon les dégradations i et domaines de confiance à 95% et à 99% (pointillés)

12.2.1.3 Caractérisation de la classe w_2

Soit x, suite de w_2 non issue de s. $C\hat{(\tau)} = \sum_{k=0}^{n-1} x_k s_{k+\tau}$. La suite x est indépendante de s, on la suppose centrée. On a donc :

$$E(C\hat{(\tau)}) = 0 \tag{12.19}$$

$$\sigma^2(C\hat{(\tau)}) = n \tag{12.20}$$

12.2.2 Calculs des probabilités d'erreurs

Notations : La fonction d'erreur sera notée erf : $erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-u^2} du$ et $erfc$, sa complémentaire sur $\mathbf{R}^+$, $erfc(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-u^2} du$

Probabilité de fausses alarmes Nous appliquons les statistiques de w_2 à l'équation 12.2. On obtient la relation suivante :

$$P_{e2}(i,d) = \frac{1}{31}\frac{1}{2}\text{erfc}(\frac{d}{\sqrt{2}\sigma_2})(1 - \frac{1}{2}\text{erfc}(\frac{d}{\sqrt{2}\sigma_2}))^{n-1} \tag{12.21}$$

La figure 12.9 présente les résultats obtenus en fonction de la valeur du seuil de décision d. On remarque que la probabilité de fausses alarmes est toujours inférieure à 0.04%. Si l'on désire avoir $P_{e2} \leq 0.01\%$, il faut prendre $d \geq 15.05$.

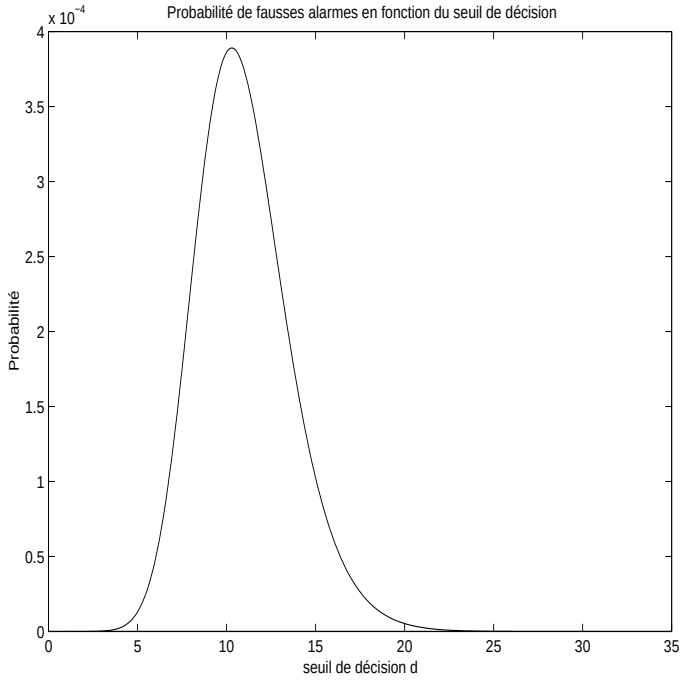


FIG. 12.9 – Probabilités de fausses alarmes

Probabilité de manque à la détection Nous appliquons les statistiques de w_1 à l'équation 12.1. On obtient la relation suivante :

$$P_{e1}(i,d) = \frac{1}{2}(1 - \frac{n-2i-d}{|n-2i-d|}) + \frac{1}{2}erfc(\frac{d-m_1}{\sqrt{2}\sigma_1}) \tag{12.22}$$

La figure 12.10 présente les résultats obtenus selon le seuil de décision d et le nombre de dégradations i, pour une m-séquence de longueur 31. La figure 12.11 présente ces mêmes résultats pour $i < 15$.

Si l'on reprend les résultats concernant la probabilité de faux positif : $P_{e2} \leq 0.01\%$ pour $d \geq 15,05$. La probabilité de manque à la détection est alors $P_{e1} \leq 0.01\%$ si $i \leq 5$.

12.2.3 Conclusion

Pour conclure nous allons comparer l'emploi des m-séquences pour le tatouage avec la méthode de détection dont nous nous sommes servis jusqu'à présent.

Dans la méthode de détection expliquée lors de la troisième partie de ce rapport, nous utilisons la distance de Hamming que nous seuillons grâce à un seuil d_0 pour obtenir la décision finale. Le calcul des erreurs de première et seconde espèce est alors donné par les relations suivantes.
Nous considérons ici une séquence aléatoire de longueur 32.

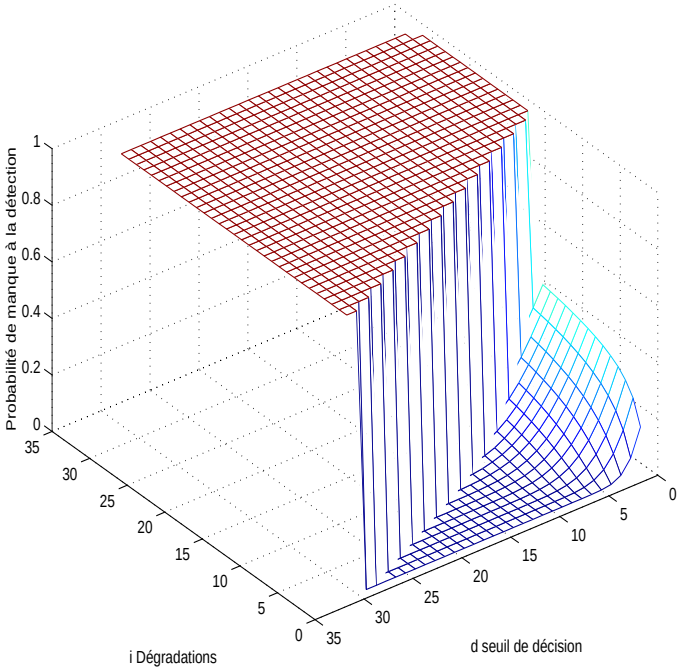


FIG. 12.10 – Probabilité de manque à la détection

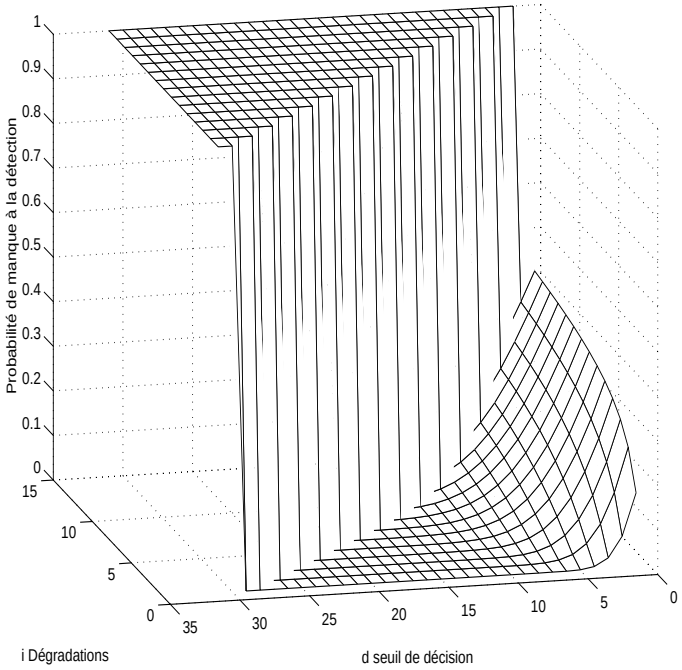


FIG. 12.11 – Probabilité de manque à la détection

Soit $d_0 = \frac{e}{32}$ où e est un entier inférieur à 32. Le nombre de fausses alarmes est donnée par l'équation suivante :

$$P_{e2} = \frac{\sum_{k=1}^{e} C_e^{32}}{2^{32}} \tag{12.23}$$

Ce nombre est fortement croissant en fonction de e, on a $P_{e2} = 0.001\%$ pour $e = 5$, $P_{e2} = 0.02\%$ pour $e = 6$ et $P_{e2} = 0.1\%$ pour $e = 7$.
Les manques à la détection sont caractérisés comme suit :

$$\begin{aligned} P_{e1}(i, d_0) &= 0 \quad \text{si } i \leq e \\ &= 1 \quad \text{sinon .} \end{aligned}$$

On détecte la marque si les altérations sont inférieures à e.

Il est difficile de comparer les deux méthodes présentées ici puisque la m-suite permet de transmettre 5 bits (l'état initial du registre de la m-séquence) et l'autre méthode permet de transmettre 32 bits. On accompagne souvent la seconde méthode de redondance. Elle permet de diminuer la probabilité de manque à la détection et ainsi d'obtenir (via le choix d'un petit seuil de détection d_0) moins de fausses alarmes à la détection. Nous comparons ci-dessous un détecteur fondé sur la méthode de détection par m-séquence au détecteur utilisant la mesure de distance de Hamming et amélioré par redondance pour la transmission de séquences de même longueur.

Considérons maintenant deux détecteurs, le premier D_1 permet de détecter 35 bits. Il détecte consécutivement 7 M-séquences de longueur 31. Si l'on fixe la probabilité de fausses alarmes $P_{e2} < 0.02\%$, $d > 13.5$, on a une détection telle que $P_{e1} < 0.01\%$ pour toutes dégradations $i \leq 3.5$ bits par séquence. La détection sera bonne pour un total de 24.5 erreurs sur les 217 réellement transmis.
Le second détecteur D_2 permet aussi de détecter 35 bits. La méthode utilisée est la distance de Hamming. La séquence analysée est de longueur 35 et est répétée 6 fois par redondance. La longueur totale de la marque est 210 bits. Pour une probabilité de faux positif fixée à $P_{e2} < 0.02\%$, $e \geq 6$. La détection sera parfaite si la séquence est dégradée de 6 erreurs maximum par séquence de 35 bits. Supposons pour simplifier le calcul qu'un coefficient de redondance de r permette de corriger r erreurs (cette hypothèse simplificatrice n'est en général pas vérifiée). En utilisant D_2 on pourra alors faire au plus 36 erreurs sur la séquence totale.

Nous pouvons alors conclure que si l'on transmet la même longueur de message, le détecteur utilisant la redondance permet d'obtenir de meilleurs résultats que celui fonctionnant avec des m-séquences.

Cinquième partie

Analyse de la méthode proposée

Chapitre 13

Analyse par les moindres carrés

Nous proposons dans ce chapitre d'analyser la méthode de tatouage par paquets d'ondelettes en utilisant comme mesure de distorsion la norme L_2. Dans la première partie de ce chapitre nous montrerons que les distorsions subies par l'image hôte lors du tatouage minimisent cette mesure. Puis nous présenterons une étude statistique permettant de quantifier les distorsions qu'un pirate doit faire subir à l'image afin de brouiller la lecture de la marque. Nous conclurons ce chapitre en présentant une méthode permettant un tatouage à deux «niveaux» de l'image. Dans cette nouvelle méthode, la marque peut être détectée avec une clef publique ou avec une clef privée. Un pirate peut invalider la détection publique mais ne peut pas enlever la marque lue avec la clef privée à moins de faire apparaître des distorsions sur l'image.

13.1 Une dégradation optimale

Soit $C_i(k,l)$ les coefficients en paquets d'ondelettes du noeud N_i, i étant le multi-indice représentant le niveau de résolution et la bande de fréquence du noeuds, B^* est la meilleure base obtenue après tatouage de l'image.

Notons D la mesure de distorsion au sens des moindres carrés. L'énergie étant conservée par la décomposition de l'image sur une base de paquets d'ondelettes, les images originale I et tatouée I^* respectent les relations suivantes :

$$D(I,I^*) = \|I - I^*\|_2^2 = \sum_{i \in B^*} \|(C_i - C_i^*)\|_2^2 \tag{13.1}$$

$$D(I,I^*) = \sum_{i \in B^*} (\|C_i\|_2^2 + \|C_i^*\|_2^2 - 2C_i^{*T} C_i) \tag{13.2}$$

Nous modifions les coefficients en paquets d'ondelettes lors de deux étapes : l'étape préliminaire consistant à stabiliser la base (voir le chapitre 9) et l'étape de tatouage de la marque (voir le paragraphe 6.2.3). Le but de ces étapes est d'augmenter l'énergie des paquets en l'amplifiant par une valeur fixée par l'algorithme. Si le noeud N_i est modifié par tatouage, $\|C_i^*(k,l)\|_2^2 = s + \varepsilon$.

Les énergies $\|C_i^*(k,l)\|_2^2$ étant fixées par la méthode, l'équation 13.2 implique que $D(I, I^*)$ sera minimum si le produit scalaire entre les matrices de coefficients en paquets d'ondelettes est maximum. La solution optimum est donc de prendre des matrices colinéaires. Ceci correspond bien à la solution que nous avons retenue (équation 6.11), *i.e.* $C_i^* = \alpha_i C_i$.

13.2 Analyse statistique

13.2.1 Schématisation

Dans l'article [42], Chen *et al.* présentent une analyse statistique de leur méthode. Ils modélisent le problème comme présenté à la figure 13.1.

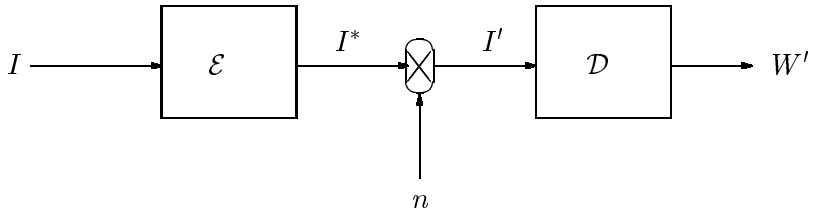


FIG. 13.1 – Schéma de détection de la marque

L'entrée du système est un signal hôte I, le message implanté pendant l'étape $\mathcal{E}$ est W. Le signal marqué est appelé I^*. L'effet de toute transformation sur le signal est modélisé par l'ajout d'un bruit déterministe ou aléatoire, dépendant ou indépendant du signal noté n. Ainsi le signal transmis est I', avec $I' = I^* + n$. Après décodage (l'étape $\mathcal{D}$ du schéma), la marque extraite est appelée W'.

13.2.2 Description de l'analyse

Soit D_{I^*} l'espérance de la distorsion entre I et I^* et $D_{I'}$ la distorsion minimum obligatoire entre I' et I qu'un attaquant doit engendrer si il veut produire une erreur de décodage de 1 bit. $\frac{D_{I'}}{D_{I^*}}$ est appelé pénalité de distorsion.

Avec ces définitions, on peut jauger les algorithmes de tatouages : si $D_{I'} >> D_{I^*}$, l'attaquant détériore fortement l'image comparée à son originale et comparée à la distorsion d'encodage de la marque.

Nous allons analyser notre processus selon cette méthode.

13.2.3 Analyse de la dégradation

Dans cette étude, on négligera l'étape de stabilisation de la structure de la base. Nous reprenons les mêmes notations qu'au chapitre 11 : la base B^* est composée de deux sous

ensembles SB^*_{nonmod} et SB^*_{mod} représentant les ensembles de noeuds non modifiés et modifiés par le tatouage. La distorsion est alors :

$$D(I, I^*) = \sum_{i \in SB^*_{mod}} \|C_i - \frac{\sqrt{s+\varepsilon}}{\|C_i\|_2} C_i\|_2^2 \tag{13.3}$$

$$D(I, I^*) = \sum_{i \in SB^*_{mod}} (\|C_i\|_2 - \sqrt{s+\varepsilon})^2 \tag{13.4}$$

On considère les valeurs $\|C_i\|_2$ comme des variables aléatoires. Pour simplifier le problème, on considérera que ces valeurs sont uniformément réparties entre 0 et $\sqrt{s}$. L'espérance de la dégradation de l'image est alors donnée par l'équation suivante

$$D_{I^*} = E(D(I, I^*)) = \sum_{i \in SB^*_{mod}} E(\|C_i\|_2^2) + (s+\varepsilon) - 2\sqrt{s+\varepsilon} E(\|C_i\|_2) \tag{13.5}$$

C'est à dire :

$$D_{I^*} = |SB^*_{mod}|(\frac{4s}{3} + \varepsilon - \sqrt{s(s+\varepsilon)}) \tag{13.6}$$

où $|SB^*_{mod}|$ est le nombre de noeuds que l'on modifie pour tatouer l'image. Dans notre cas, on fait environ trois modifications pour implanter 1 bit à 1 de la marque. Si m est la longueur de la marque, $|SB^*_{mod}| \approx 3m/2$. On aura alors

$$D_{I^*} = \frac{3m}{2}(\frac{4s}{3} + \varepsilon - \sqrt{s(s+\varepsilon)}) \tag{13.7}$$

Si l'on prend comme valeurs $s = 10^{-5}$, $\varepsilon = 3s$ et $m = 7 * 32$, ce qui constitue un très fort tatouage, on a $D_{I^*} = 7.8.10^{-3}$.

13.2.4 Une attaque optimale : l'inversion du tatouage

L'attaquant veut trouver l'opération de distorsion minimale (c'est à dire le bruit n qui minimise $D(I, I')$) et qui perturbe la base modifiée B^* pour faire un bit d'erreur. On calcule donc :

$$D(I, I') = \|I^* + n - I\|_2^2 \tag{13.8}$$

$$D(I, I') = D(I, I^*) + \|n\|_2^2 + 2n^T(I^* - I) \tag{13.9}$$

On trouve que la transformation optimale est la transformation triviale qui inverse le marquage. L'opération s'écrit :

$$\tilde{n} = E(n/I^*) = E(I/I^*) - I^* \tag{13.10}$$

où $E(X/Y)$ est l'espérance de X sachant Y. Le pirate doit donc estimer la marque, ce qui revient à estimer l'image originale connaissant l'image tatouée.

Bien que dans notre méthode, la clef privé soit confidentielle, nous allons nous intéresser au cas où le pirate connaît toutes les informations : l'algorithme, la clef, la marque et le seuil de détection sont connu. On se place alors dans le cas le plus défavorable, on étudie notre méthode comme si elle était à clef publique. Nous calculerons alors les erreurs que l'attaquant fait lorsqu'il estime la marque, puis nous donnerons une solution à cette attaque.

13.2.4.1 Algorithme à clef publique

L'objectif du pirate dans ce paragraphe est de trouver une image I' qui se rapproche le plus possible de l'image originale. La meilleure façon de procéder est d'inverser le tatouage, c'est à dire d'inverser l'étape de modification des coefficients en paquets d'ondelettes.

Le pirate connaît la clef, il connaît alors la structure de la base B (qu'il retrouve grâce à B^*, la clef et ses connaissances sur l'algorithme d'implémentation de la marque). Il connaît donc l'emplacement des noeuds qui ont été exclus par tatouage. Appelons ces noeuds SB_{mod}. Son objectif est de restaurer la présence de ces noeuds dans la meilleure base de l'image I' résultat de l'inversion du tatouage.

Estimation des coefficients en paquets d'ondelettes Pour chaque noeud N_p de SB_{mod} qu'il doit restaurer, le pirate (appelons le Bob) se trouve face à 4 fils d'énergie supérieure à s sélectionnés par B^*. Pour que N_p soit à nouveau sélectionné par la meilleure base, Bob doit diminuer l'énergie de l'un des 4 fils de N_p. Il ne sait pas si les énergies de ces noeuds ont été modifiés par Alice (la propriétaire de l'image originale). Pour faire le tatouage, Alice a du modifier en moyenne 3 fils par noeuds de SB_{mod}. Ces noeuds (fils) modifiés par Alice appartiennent au sous ensembles SB^*_{mod}.

Bob choisit un noeud N_i qu'il considère modifié par le tatouage, l'expression de ses coefficients respecte alors l'équation des modifications rappelée ci-dessous :

$$C_i^* = \frac{\sqrt{s+\varepsilon}}{\|C_i\|_2} C_i \tag{13.11}$$

ainsi pour estimer C_i sachant C_i^*, il suffit d'estimer la norme $\|C_i\|_2$:

Une hypothèse raisonnable que fait alors Bob est que les $\|C_i\|$ sont répartis uniformément sur l'intervalle $[0, \sqrt{s}]$, le pirate peut alors choisir la norme des coefficients qu'il désire obtenir :

$$\|C_i'\|_2 = E(\|C_i\|_2) = \frac{\sqrt{s}}{2} \tag{13.12}$$

Une foi la norme estimée, le pirate calcule les coefficients selon l'équation suivante :

$$C_i' = \frac{\sqrt{s}}{2} \frac{C_i^*}{\|C_i^*\|_2} \tag{13.13}$$

La relation 13.11 implique

$$C_i' = \frac{\sqrt{s}}{2} \frac{C_i}{\|C_i\|} \tag{13.14}$$

On peut remarquer ici que la connaissance de ε n'est pas nécessaire pour calculer les coefficients C'_i.

L'objectif du paragraphe suivant est de calculer les erreurs de distorsions que ce choix des coefficients induit sur l'image I'.

Distorsion Considérons dans un premier cas que Bob ait fait le bon choix en modifiant le noeud N_i. C'est à dire $N_i \in SB^*_{mod}$. La distorsion est alors donnée par :

$$D_{I'1} = E(D_1(I, I')) = E(\frac{\sqrt{s}}{2} - \|C_i\|_2)^2 \tag{13.15}$$

$$D_{I'1} = E(D_1(I, I')) = \frac{s}{12} \tag{13.16}$$

Si le noeud choisi par Bob ne fait pas partie de ceux qui ont été modifiés au marquage, son énergie est $\|C_i\| \approx \sqrt{s+\varepsilon}$ (Bob l'a confondu avec un noeud modifié). Le coût de la transformation est alors :

$$D_{I'2} = D_2(I, I') = (\frac{\sqrt{s}}{2} - \sqrt{s+\varepsilon})^2 \tag{13.17}$$

$$D_{I'2} = \frac{5s}{4} + \varepsilon - \sqrt{s(s+\varepsilon)} \tag{13.18}$$

Soit P_1 la probabilité que Bob choisisse un noeud modifié par Alice, alors la distorsion minimale commise par Bob pour faire i erreurs dans le tatouage d'Alice est donnée par la relation suivante :

$$D_{I'}(i) = i(P_1 D_{I'1} + (1 - P_1) D_{I'2}) \tag{13.19}$$

En général, on modifie 3 fils pour exclure un noeuds : $P_1 = \frac{3}{4}$. La distorsion devient alors :

$$D_{I'}(i) = i(\frac{3s}{8} + \frac{\varepsilon - \sqrt{s(s+\varepsilon)}}{4}) \tag{13.20}$$

Le rapport de pénalité de distorsion est donc :

$$\frac{D_{I'}(i)}{D_{I^*}} = \frac{i(3s + 2(\varepsilon - \sqrt{s(s+\varepsilon)}))}{m(16s + 12(\varepsilon - \sqrt{s(s+\varepsilon)}))} \tag{13.21}$$

Si l'on pose $\varepsilon = \xi s$, alors le rapport de pénalité de distorsion est indépendant de s et respecte l'équation suivante :

$$\frac{D_{I'}(i)}{D_{I^*}} = \frac{i(3 + 2(\xi - \sqrt{1+\xi}))}{m(16 + 12(\xi - \sqrt{1+\xi}))} \tag{13.22}$$

Le rapport de distorsion est une fonction décroissante de ξ avec :

$$\frac{1}{12}\frac{i}{m} \leq \frac{D_{I'}(i)}{D_{I^*}} \leq \frac{1}{8}\frac{i}{m} \tag{13.23}$$

Cette dernière équation signifie que quel que soit le choix de ε, Bob pourra se rapprocher de l'image originale en invalidant le marquage. Par cette méthode Bob peut invalider $i = m/2$ bits de la marque (il ne peut que modifier les 1 en 0). La distorsion que Bob fait alors est au plus 8 fois moins importante que celle que fait Alice en tatouant l'image. Cette attaque est donc concluante. Cependant, nous avons fait l'hypothèse de départ que le pirate connaissait la clef secrète, ce qui ne doit pas être le cas dans la réalité. D'autre part, même dans ce cas extrême, il existe une solution à cette attaque, que nous présentons au paragraphe suivant.

13.2.5 Solution à cette attaque : la méthode par «leurres»

Afin d'être robuste à cette attaque, nous avons développé une variante à la méthode de tatouage par paquets d'ondelettes. Nous allons maintenant expliquer cette nouvelle méthode que nous appellerons méthode *par leurre* .

13.2.5.1 Principe de la méthode par leurre

Le principe de la méthode par leurre est d'obliger le pirate à faire beaucoup d'erreurs de type $D_{I'2}$. Pour cela, il suffit de cacher les noeuds exclus (appartenant à SB_{mod}) dans un ensemble de noeuds.

Rappelons tout d'abord qu'à la détection, l'extraction de la watermarque $W' = (W_i)_{i=1..m}$ peut se faire de différentes façons dont l'une consiste à compter les noeuds pointés par $K = (K_i)_{i=1..m}$ et présents dans B^* selon l'équation 6.10 que l'on répète ci-dessous :

$$W'_i = |K_i(B^*)| \text{ modulo}(2) \tag{13.24}$$

Avec les notations définies ci-dessus, l'ensemble des noeuds exclus de la base est : $SB_{mod} = K(B) - K(B^*)$ où l'opérateur «$-$» signifie «sans».

Dans l'attaque par inversion, le pirate retrouve les noeuds exclus par l'opération suivante :

$$SB_{mod} = K(A) - K(B^*) \tag{13.25}$$

où A représente l'arbre de décomposition en paquets d'ondelettes.

Le principe de la méthode par leurre est de construire une clef publique K_n permettant de détecter la présence de la marque mais ne permettant pas à un attaquant d'enlever la marque. L'idée principale de cette méthode est que la clef publique K_n pointe un p-uplets de noeuds à la place d'un couple de noeuds par bit de la marque. Le paragraphe suivant présente la construction de cette clef publique K_n.

13.2.5.2 Obtention de la clef publique de détection

La méthode de tatouage par paquets d'ondelettes ne change pas. la clef K est construite comme expliqué auparavant.

L'idée de la méthode des leurres est de créer une nouvelle clef K^n, qui contienne les informations de K et des informations de «leurres» données par une clef K^l. Ainsi la nouvelle clef K^n ne sera plus composée de couples de pointeurs sur les noeuds mais de p-uplets de pointeurs. Nous expliquons ici la construction de K^n et ses effets sur l'attaque d'inversion et la détection de la marque.

Soit une clef K^l composée de pointeurs sur des paquets appartenant à l'arbre A et n'appartenant pas à la base B^*. Cette clef définit le sous ensemble de noeuds de l'arbre SE_{leurre}. Formellement, on peut écrire :

$$SE_{leurre} = K^l(A) = K^l(A) - K^l(B^*) \tag{13.26}$$

On appelle cet ensemble SE_{leurre} car il est composé de noeuds qui ne sont pas utilisé lors de la détection mais qui tromperont le pirate.

Soit alors la nouvelle clef de détection K^n avec $K^n = K \bigcup K^l$. Le pirate possédant la clef complétée K^n aura accès à

$$SE_{accs} = K^n(A) - K^n(B^*) = K(A) - K(B^*) + K^l(A) - K^l(B^*) = SB_{mod} \bigcup SE_{leurre} \tag{13.27}$$

où «+» signifie «union».

Le pirate n'a donc plus accès à l'ensemble des noeuds exclus.

Regardons comment se déroule la détection pour le bit i de la marque :

$$\begin{aligned} W_i^l &= |K_i^n(B^*)| \text{ modulo}(2) \\ &= |K_i^l(B^*) + K_i(B^*)| \text{ modulo}(2) \\ &= |K_i(B^*)| \text{ modulo}(2) \\ &= W_i' \end{aligned} \tag{13.28}$$

La détection se déroule comme auparavant, tous les possesseurs de K_n peuvent lire et détecter la marque.

Il est évident que le pirate peut utiliser la méthode d'inversion pour invalider la détection publique par la clef K_n. Il lui suffit pour cela de faire apparaître les noeuds de l'ensemble SE_{accs} dans la meilleure base B' d'une image I' obtenue à partir de I. Cependant, il fera alors des erreurs de type $D_{I'2}$ qui éloignerons I' de I et de plus il ne sera pas sûr d'avoir invalidé la détection de la marque avec la clef privée K. Nous allons calculer dans le prochain paragraphe le nombre de noeuds de «leurre» que doit pointer la clef publique pour que l'attaque par inversion soit trop coûteuse en terme de distorsion.

13.2.5.3 Inversion du tatouage par leurre

Soit x, le nombre de noeuds de leurres pointés par chacune des clef K_i^l : $x = |K_i^l(A)|$ (on suppose que ce nombre est constant). Si Bob veut être certain de modifier i valeurs de la marque extraite, il produit sur l'image I' obtenue par inversion la distorsion suivante :

$$D_{I'l}(i) = i(P_1 D_{I'1} + (1 - P_1)D_{I'2} + xD_{I'2}) \tag{13.29}$$

ce qui nous donne une pénalité de :

$$\frac{D_{I'l}(i)}{D_{I^*}} = \frac{D_{I'}(i)}{D_{I^*}} + ix\frac{D_{I'2}}{D_{I^*}} \tag{13.30}$$

Cette pénalité est positive si :

$$x > \frac{D_{I^*}}{iD_{I'2}}(1 - \frac{D_{I'}(i)}{D_{I^*}}) \tag{13.31}$$

C'est à dire si :

$$x > \frac{3m}{i}\frac{4}{3}(1 - \frac{i}{m}\frac{1}{4}) \tag{13.32}$$

Enfin, on a :

$$x > \frac{4m}{i} - 1 \tag{13.33}$$

Si le pirate veut enlever tout le code, il devra faire $i = m/2$ erreurs. Cela sera impossible sans faire de distorsions, si l'on a auparavant pris la sécurité de compléter la clef avec 7 noeuds de leurre pour chaque sous-base. Si le pirate veut faire $i = m/4$ erreurs dans la détection de la marque, l'attaque produira des distorsions sur l'image à condition que l'on ait complété la marque avec 15 noeuds de leurres par sous-base.

Les noeuds de leurre étant pris n'importe où dans l'arbre de décomposition en paquets d'ondelettes A, on peut en choisir un très grand nombre sans contraintes.

La méthode de tatouage par leurres est une méthode à deux niveaux : deux tatouages sont contenus dans le même. Un tatouage clef publique est fragile (a l'attaque illicite d'inversion de la marque) et un tatouage à clef privé qui est robuste à cette attaque (si l'on a pris la précaution de donner une clef publique assez complexe).

Nous allons maintenant étudier une autre attaque maligne : l'attaque de surmarquage.

13.2.6 Une autre attaque illicite : le surmarquage

Nous supposons qu'un pirate veuille détruire la marque par surmarquage. Son but est de modifier la structure de la base en appliquant la même méthode que celle de tatouage par paquets d'ondelettes. L'objectif de Bob est d'exclure de la meilleure base de l'image I', les noeuds pointés par K et appartenant à B^*.

Nous supposons ici que Bob connaît la clef K de marquage, il connaît donc les noeuds à modifier. Chacune des modifications que fait Bob produira une erreur dans le tatouage

d'Alice. Pour invalider tout le code, Bob fait une modification sur chaque sous-base. Soit i, le nombre d'erreur que Bob veut faire au tatouage d'Alice, les dégradations que l'image subie sont alors en espérance :

$$E(D(I^*, I')) = 3i(\frac{4s}{3} + \varepsilon - \sqrt{s(s+\varepsilon)}) \tag{13.34}$$

Les modifications entraînées par le tatouage d'Alice et l'attaque de Bob sont orthogonales, on a donc :

$$D(I, I') = D(I, I^*) + D(I^*, I') \tag{13.35}$$

On peut ajouter Bob a moins de choix qu'Alice sur les noeuds à modifier, si Bob fait le même nombre de modifications qu'Alice, on a $D(I, I^*) < D(I^*, I') < D(I, I')$.

Cette attaque n'est donc pas dangereuse pour notre méthode car elle dégrade l'image (si l'on choisit la norme L_2 comme mesure de distorsion). Cependant, Bob détruit ainsi le nombre de bits de la marque qu'il veut. Pour éviter cela, on peut utiliser une méthode par leurre. De même que pour l'attaque d'inversion, il suffit de compléter la clef K par une clef K_l. K_l pointe sur un nombre pair de noeuds de B^* : la détection modulo(2) n'est pas affectée et le pirate ne peut invalider la détection de W avec la clef K qu'au prix d'un grand nombre de modifications.

Chapitre 14

Structure de la clef K

Dans ce chapitre, nous allons généraliser la structure de la clef K que nous avons choisie lors de la troisième partie. Nous définirons les paramètres qui permettent de choisir la clef puis nous étudierons les influences de ces paramètres sur la méthode. Nous justifierons alors le choix de la structure de la clef que nous avons défini à la troisième partie.

14.1 Schématisation et notations

La méthode de tatouage par paquet d'ondelettes peut être schématisée d'une façon complètement différente de celle effectuée au chapitre 6. Les différentes étapes de l'implémentation de la marque sont représentés figures 14.1 à 14.6. Chacune des étapes est expliquée ci dessous.

Étape 1

La figure 14.1 présente la première étape du tatouage. La meilleure base B est sélectionnée. On la présente ici comme un flux de noeuds. On parcoure l'arbre de haut en bas (à résolution fréquentielle croissante) et de droite à gauche à bande de fréquences centrales croissantes. Sur la figure, les noeuds sélectionnés dans la base sont représentés par des carrés vides, les noeuds qui ne sont pas dans B sont représentés par des croix (leurs descendants seront sélectionnés dans B). Dans ce flux, on note 1 les noeuds de B et 0 les noeuds de l'arbre qui ne sont pas sélectionnés par B. La taille de l'arbre est $\frac{1}{3}(4^m - 1)$.

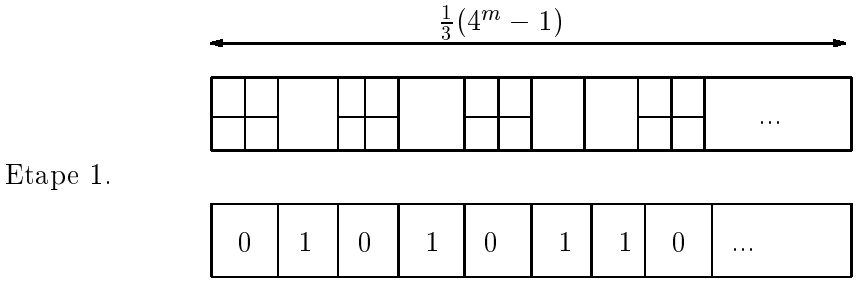


FIG. 14.1 – Schématisation du tatouage, représentations des noeuds de B

Étape 2

Parmi le flux de valeurs obtenu à l'étape 1, on ne considère que les noeuds portant la valeur «1», c'est à dire ceux de B. De plus, on ne considère que les noeuds susceptibles d'être marqués : les noeuds des premiers niveaux et du dernier sont éliminés. Dans la mesure où cette information est publique, ces noeuds n'auront aucune incidence dans les études suivantes, qu'il s'agisse de marquage ou d'attaque.
On a ainsi un flux de valeurs ne dépendant que de l'image et de la meilleure base. La figure 14.2 présente ce flux constitué de N_B noeuds de valeur «1».

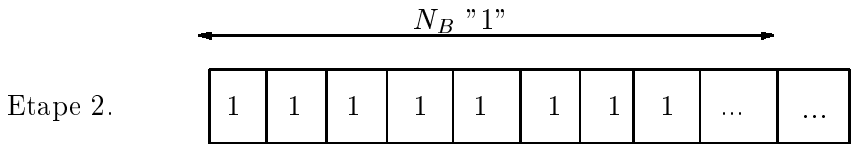


FIG. 14.2 – Représentation des noeuds de B susceptibles d'être marqués

Étape 3

La figure 14.3 illustre la troisième étape. On sélectionne une proportion de RN_B noeuds parmi les N_B noeuds. Ce nouveaux flux de noeuds sera pointé par la clef K. On a précédemment appelé ces noeuds $SB = K(B)$. Les $(1 - R)N_B$ noeuds restant ne serviront pas au tatouage.

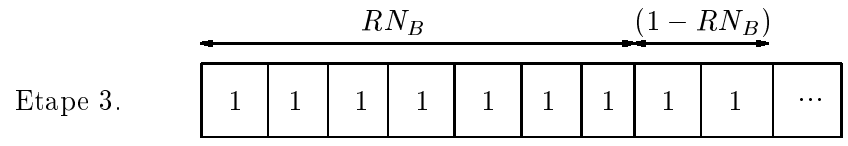


FIG. 14.3 – Représentation des noeuds pointés K

Étape 4

La quatrième étape (voir la figure 14.4) consiste à créer à partir du flux précédent des m sous ensembles de cardinal p. Ce seront les sous-bases $\{SB_i\}_{i=1..m}$. Dans la méthode présentée à la partie 3, $p = 2$. Ces sous-bases sont sélectionnées par la clef K avec $SB_i = K_i(B)$. Nous ne traitons pas ici le cas où les sous bases ne sont pas disjointes bien que ce soit un cas intéressant.

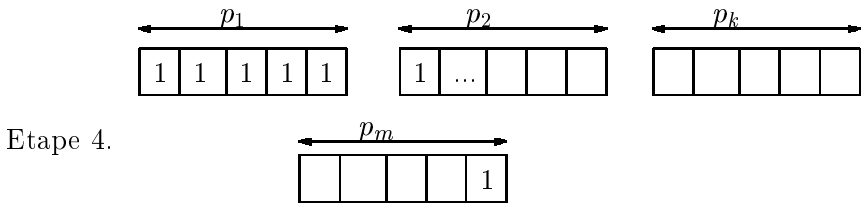


FIG. 14.4 – Représentations des noeuds pointés K_i

Étape 5

L'étape 5 est la modification de la structure de chaque sous-base par tatouage. Chaque sous-base SB_i porte la valeur d'un élément de la marque $W = (W_i)_{i=1..m}$. Nous insistons sur le fait que dans ce paragraphe, W_i n'est plus binaire. On exprime W_i en base b ou b est un entier supérieur à 2. W_i indique le nombre de noeuds qui resteront dans SB_i^* après modifications : On aura $W_i = |K_i(SB_i^*)|$ modulo(b). Par exemple, il restera dans la première sous-base de la figure 14.5 $W_1 = 2$ noeuds sur les 5 présents au départ (si on prend $b > 2$). N_m est le nombre de modifications faites sur le flux, c'est le cardinal de l'ensemble des noeuds exclus appelé SB_{mod}

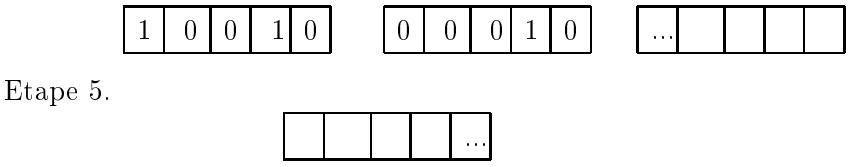


FIG. 14.5 – Représentations des noeuds exclus $K_i(SB^*)$

Étape 6

L'étape 6 est la réintégration des sous-bases modifiées SB^* dans la base qui devient ainsi B^*. Les noeuds de SB_{mod} sont remplacés par leurs fils. Il y aura $4N_m$ nouveaux noeuds crées dans la structure de B^*. Dans la figure 14.6, les noeuds sont réintégrés dans le flux premier qui représente l'arbre de décomposition (dans le désordre). Les N_B premiers noeuds sont ceux de B, les «0» représentant les noeuds modifiés. La seconde figure présente la structure de l'arbre de décomposition présenté comme pour la première étape. Sur ce flux, il y a $RN_B - N_m$ noeuds inchangés (ils appartiennent à $B \bigcap B^*$), et

$4N_m$ nouveaux noeuds. Parmi ces derniers, il y a ceux dont l'énergie à été modifiée on note leur ensemble SB^*_{mod}. Les autres noeuds ne sont pas considérés par le tatouage.

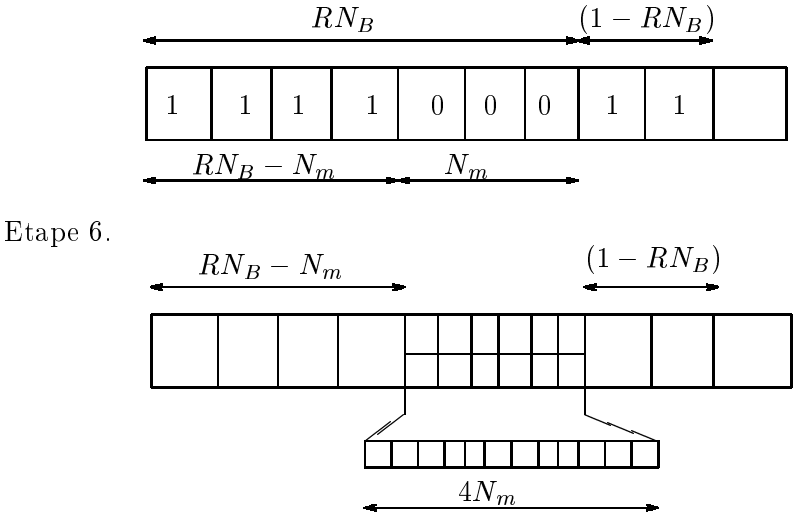


FIG. 14.6 – Représentations des noeuds de B^*

A travers cette modélisation, les paramètres de la méthode apparaissent mieux. N_B étant fixé par la structure de la base B (c'est à dire par s le seuil de sélection), il faut déterminer : le pourcentage R de noeuds pointés par K, le cardinal p de chaque sous-base ainsi que b la base sur laquelle nous allons écrire la marque.

14.2 Paramètres en sortie

Nous allons définir ici des coefficients qui permettront d'appréhender les performances de la méthode. Nous considérons une image I et une clef K fixées.

- m est la taille de la marque (y compris redondance et code correcteurs d'erreurs). Elle est exprimée en unité de message (nombre de bits, nombre de digits ...).
- N_m est le nombre «moyen» de modifications. C'est le nombre de noeuds de SB_{mod} : le nombre de noeuds exclus. Il est calculé pour une watermarque «moyenne».
- N_c est le nombre de choix que l'on a sur les noeuds à exclure. Dans chaque sous-bases, il y en effet plus de noeuds présents que de noeuds à exclure, N_c donne le nombre de ces choix. On l'exprime en nombre de noeuds par sous-bases.

Le tableau 14.1 présente les paramètres de sortie que nous avons défini ci-dessus et leurs rôles respectifs dans le processus de tatouage.

14.3 Actions des paramètres d'entrée sur la sortie

Nous allons étudier dans les paragraphes suivants les influences des choix des paramètres p, b, R sur les coefficients de sorties m, N_m et N_c.

TAB. 14.1 – Paramètres de sortie

paramètre	description	rôle	optimisation
m	taille de la marque	détection	maximiser
N_m	nombre moyen de modifications	invisibilité	minimiser
N_c	nombre de choix sur les modifications	invisibilité/robustesse	maximiser

14.3.0.1 Choix de p

Commençons par étudier les influences du choix du paramètre p sur la méthode. Pour cela, nous prenons b fixé. Rappelons que b est la base sur laquelle nous exprimons la marque. Par exemple, si $b = 2$: la marque est binaire, si $b = 10$, les vecteurs de la marques seront des chiffres de 0 à 9. p est le cardinal de chaque sous-base. Le problème que nous posons ici est donc combien faut-il de noeuds pour exprimer un nombre «modulo (p)». Nous avons dégagé les trois cas ci-dessous :

- Cas (1) : $p = b - 1$. Le nombre de noeuds dans SB_i est le minimum requis pour exprimer un nombre appartenant à $[0..b-1]$. L'opérateur «modulo» ne sera plus utile à la détection.
- Cas (2) : $p = b$. On a un noeud de plus dans les sous-bases qu'au cas précédent.
- Cas (3) : $p = k(b-1)$. La sous-base contient beaucoup plus de noeuds qu'il n'en faut. Ce choix permet par exemple de maximiser N_c.

Les paramètres de sortie calculés pour ces différents choix porteront les indices respectivement 1, 2 et 3.

a) Influence sur la taille de la marque m Pour les trois cas on a $N_B R = mp$, ce qui donne pour chacun des cas :

- $m_1 = \frac{N_B R}{b-1}$
- $m_2 = \frac{N_B R}{b}$ et $\frac{m_2}{m_1} = 1 - \frac{1}{b}$
- $m_3 = \frac{N_B R}{k(b-1)}$

On a ainsi $\forall b, m_1 > m_2 \geq m_3$. Il est évident que m_3 est alors le plus mauvais choix.

b) Influence sur le nombre moyen de modifications La watermarque W_i est exprimée en base b, c'est à dire que W_i est à valeur dans $[0..b-1]$. Soit $V_i = |K_i(SB_i^*)|$, on a directement $W_i = V_i$ modulo(b). V_i est le nombre de noeuds non exclus de SB_i. La définition de V_i change en fonction de p et influence directement le nombre des modifications. Nous détaillons ci-dessous les différents cas, et nous prenons pour cela une watermarque «moyenne» $E(W_i)$. W_i est uniformément distribuée sur $[0..b-1]$, son espérance est : $E(w_i) = \frac{b-1}{2}$. V_i sera le nombre de noeuds restant dans la sous-base pour cette marque moyenne.

- Dans le cas (1), $EV_i = E(W_i)$, le nombre moyen de noeuds modifiés par sous-base est égal à $E(W_i)$, d'où : $N_{m1} = \frac{m_1(b-1)}{2}$, d'où $N_{m1} = \frac{N_B R}{2}$. On modifie la moitié des

noeuds.
- Si $p = b$, on peut prendre V_i, $V_i = W_i + 1$ (plus V_i est grand, moins on fait de modifications). $V_i = \frac{b+1}{2}$, on trouve $N_{m2} = \frac{m_2(b-1)}{2} = \frac{N_B R}{2}(1 - \frac{1}{b})$.
- Dans le cas 3, le nombre de modifications ne change pas par rapport au premier cas. Ainsi $N_{m3} = \frac{N_B R}{2k}$

On a $\forall b, N_{m1} > N_{m2} \geq N_{m3}$.
Le premier choix est le plus mauvais. Dans le deuxième cas, N_m est minimum pour $b = 2$ et croit en fonction de b.

c) Influence sur le choix du noeud à modifier Le nombre «moyen» de choix N_c est le nombre de façon de choisir les $\frac{N_m}{m}$ noeuds modifiés parmi les p vecteurs de la sous base. p étant uniforme, N_c est constant sur chaque sous base, on prendra $N_c = C^p_{\lceil(\frac{N_m}{m})\rceil}$ où $\lceil\rceil$ est la partie supérieure. On a alors pour les différents cas étudiés :
- $N_{c1} = C^{b-1}_{\lceil\frac{b-1}{2}\rceil} = \frac{(b-1)!}{((\lceil\frac{b-1}{2}\rceil)!)^2}$
- $N_{c2} = C^{b}_{\lceil\frac{b-1}{2}\rceil} = bN_{c1}$
- $N_{c3} = C^{k(b-1)}_{\lceil\frac{b-1}{2}\rceil}$

$\forall b, N_{c3} \geq N_{c2} > N_{c1}$.
Pour $b = 2$, $Nc1 = 1$, on ne peut pas choisir le noeud à modifier. Dans ce cas, on préférera la solution du cas 2, $N_{c2} = 2$ ou celle du 3 : $N_{c3} = k_0$.

Le tableau 14.2 résume les influences des trois cas étudiés ci-dessus sur les descripteurs de la méthode. Afin de conclure sur le choix de l'un de ces trois cas, nous allons étudier au paragraphe suivant les réactions de notre méthode à une attaque de surmarquage.

TAB. 14.2 – Actions des paramètres sur les descripteurs

paramètres	m	N_m	N_c
$p = b - 1$	$\frac{N_B R}{b-1}$	$\frac{N_B R}{2}$	$C^{b-1}_{\frac{b-1}{2}}$
$p = b$	$m_1(1 - \frac{1}{b})$	$N_{m1}(1 - \frac{1}{b})$	bN_{c1}
$p = k(b-1)$	$\frac{N_B R}{k(b-1)}$	$\frac{N_B R}{2k}$	$C^{k(b-1)}_{\frac{b-1}{2}}$

14.3.0.2 Étude de l'attaque par surmarquage

Un attaquant, Bob surmarque une image déjà marquée, soit pour y mettre sa marque, soit pour invalider le marquage. Nous allons voir dans ce paragraphe comment notre tatouage résiste à une telle modification. Nous nous intéressons ici à la deuxième hypothèse, *i.e.* Bob veut invalider le tatouage.

Bob ne connaît pas la clef d'Alice, et utilise le même algorithme pour surtatouer l'image, avec les mêmes paramètres. Le tatouage d'Alice est invalidé si Bob choisit et modifie les noeuds qu'Alice a choisi de ne pas modifier.

Après le marquage d'Alice, la base B^* contient (voir les figures 14.1 à 14.6) $(1-R)N_B$ noeuds non utilisés pour le marquage, $RN_B - N_m$ noeuds non modifiés et $4N_m$ noeuds engendrés par modifications.

Bob va réaliser le surtatouage, de la même façon qu'Alice, sur les noeuds susceptibles d'être marqués. Or les noeuds de la plus grande profondeur ne sont pas considérés. Admettons qu'Alice modifie uniformément les trois avant dernières profondeurs de l'arbre. Un tiers des modifications faîtes par Alice ne seront donc pas considéré par Bob.

Le marquage de Bob produit i erreurs dans celui d'Alice, si, en N_m modifications, i noeuds parmi les $RN_B - N_m$ noeuds quantifiés sont touchés. La probabilité de faire i erreurs est donnée par : $P(i) = C^i_{N_m}(\alpha_{nm})^i(1-\alpha_{nm})^{N_m-i}$ où $\alpha_{nm} = \frac{RN_b - N_m}{N_B + \frac{5}{3}N_m}$.

Pour N_m assez grand, le binôme peut s'approximer par une gaussienne de moyenne $m_p = N_m\alpha_{nm}$ et de variance $\sigma_p^2 = N_m\alpha_{nm}(1-\alpha_{nm})$.

La probabilité pour qu'il y ait plus de $imax_1$ erreurs est donnée par :

$$P_e(imax_1) = 1/2 * (1 - \mathrm{Erf}(\frac{imax_1 - m_p}{\sqrt{2}\sigma_p}))$$

- a) Si $p = b - 1$, alors $\alpha_{nm} = \frac{1}{\frac{2}{R} + \frac{5}{3}}$. ($imax_1$ diminue avec N_B et augmente avec R). On trouve pour $N_B = 2000$ et $R > 0.5$, $24\% < imax_1 < 32\%$
- b) Si $p = b$, alors $N_m = \frac{N_B R}{2}(1 - \frac{1}{b})$ et $\alpha_{nm} = \frac{1+\frac{1}{b}}{\frac{2}{R} + \frac{5}{3}(1+\frac{1}{b})}$ Les résultats varient très peu en fonction de b et sont du même ordre.
- c) Cas $p = k(b-1)$, on obtient $\alpha_{nm} = \frac{2k-1}{\frac{2k}{R} + \frac{5}{3}}$. Les résultats sont évidement moins bons que pour les deux cas précédents. De l'ordre de 40% pour $k_0 = 2$ et de 50% pour $k_0 = 8$.

Remarque : Nous allons calculer les distorsions : Bob fait le même tatouage qu'Alice et les distorsions que font Bob et Alice sont orthogonales. On a donc, en reprenant les notations du paragraphe 13.2,

$$D(I, I') = D(I, I^*) + D(I^*, I')$$

.

14.3.0.3 Conclusion

L'étude que nous avons faite sur l'attaque de surmarquage nous permet d'éliminer le cas (3). En effet, dans ce cas, le surmarquage est une attaque très dangereuse. Le choix du premier cas permet de maximiser la taille de la marque mais donne de très mauvais résultats sur les deux coefficients N_m et N_c. la meilleure solution est donc de choisir le cas (2), *i.e.* $p = b$.

14.3.0.4 Choix de b

Nous rappelons que b est le paramètre de «modulo». Il définit la base sur laquelle nous allons exprimer notre message. Par exemple, si $b = 2$, le message est binaire, si $b = 10$ le message est exprimé en base 10. b peut être vue comme l'alphabet du codage.

a) Influence sur la marque La taille de la marque est inversement proportionnelle à b (voir 14.3.0.1). Cependant, si b est grand la marque est effectivement moins longue mais chaque unité porte plus d'informations. Pour un code W_i exprimé en base b et de longueur m, le nombre de marques possibles est b^m. Or m et b sont liés par une constante c dépendant de la base par : $mb = c$. Soit la fonction f de $[1, +\infty[$ dans $\mathbb{R}$, $f(b) = b^{c/b}$. L'étude de f montre que cette fonction à un unique maximum en $b = \exp(1)$. Pour $b \in \mathbb{Z}^*$, le maximum est atteint en $b = 3$ ($b = 2$ est le maximum suivant).

b) Influence sur le nombre de modifications Dans le cas ou $p = b$, le nombre de modifications dépend de b. L'étude de ce cas donné au paragraphe 14.3.0.1b, montre qu'alors le choix $b = 2$ est le meilleur.

c) Influence sur le nombre de choix Si l'on choisit $p = b$, le nombre de choix N_c est une suite fonction de b, avec : $N_c(b+1) = 4(1 + \frac{1}{\frac{b-1}{2}+1} N_c(b-1))$, $N_c(3) = N_c(2) = 2$. Cette suite augmente très vite avec b (en puissance de 4), ce qui nous incite à prendre b grand.

Conclusion Le choix $b = 3$ est intéressant, malgré cela, on décide de prendre $b = 2$. Le nombre de modifications N_m est alors minimisé. De plus, pour ce choix, la marque est binaire. La méthode est simplifiée, elle est homogène avec la plupart des méthodes existantes, nous pourrons alors utiliser des m-séquences pour exprimer la marque. Le principal inconvénient de ce choix concerne le coefficient N_c. Le tableau 14.3 donne les valeurs que l'on obtient avec ce choix de b.

TAB. 14.3 – Actions des paramètres sur les descripteurs

paramètres	m	N_m	N_c
$p = b = 2$	$\frac{N_B R}{2}$	$\frac{N_B R}{4}$	2

14.3.0.5 Choix de R

Le coefficient R correspond à la proportion de noeuds de B qui sont sélectionnés par la clef K. Les descripteurs m et N_m évoluant de la même manière en fonction de R, cette étude ne nous permet pas de conclure. L'attaque par surmarquage nous incite à choisir une petite valeur de R. Cependant, nous verrons au chapitre suivant que le choix d'une grande valeur de R diminue le nombre de fausses alarmes. Dans la pratique, nous choisirons une valeur moyenne de R, par exemple 2/3.

Chapitre 15

Fiabilité du processus de détection d'une marque

Lors de la présentation des attaques au chapitre 1.4.2, nous avons introduit une attaque particulière que nous avons appelée *fausses alarmes naturelles*. Cette attaque n'est pas une attaque classique car ce n'est pas une transformation de l'image. Elle peut être vue comme une attaque protocolaire. Elle est fondée sur l'observation que quelle que soit la méthode de tatouage utilisée, la détection peut être positive pour un certain nombre d'image *non tatouées*. Or le cahier des charges idéal impose que le nombre de faux positif soit nul. Nous allons étudier dans ce chapitre l'importance d'apparitions de ces fausses alarmes pour les schémas de tatouages additif ainsi que pour le schéma de tatouage par paquets d'ondelettes.

Définition et notations

Il y a fausse alarme lors du processus de détection d'une marque W si une image n'est pas marquée (ou marquée d'une autre marque W_2) et que la détection est positive. Cela peut arriver si la marque est présente à «l'état naturel» dans une image. Nous proposons dans ce chapitre d'approcher la valeur de cette erreur par des calculs simples.

Soit l'ensemble $\mathcal{I}$ des images $p \times p$ à N niveaux de gris. Le cardinal de cet ensemble est de $N_{itot} = N^{p^2}$.

15.1 Le patchwork

Soit 2 ensembles A et B formant une partition de l'image, on a $A = \{a_i\}_{i=1..p^2/2}$ et $B = \{b_i\}_{i=1..p^2/2}$. La condition de détection de la marque est donnée par : $\sum a_i - \sum b_i = p^2$.

Calculons N_{ip} le nombre d'images remplissant cette contrainte de détection, c'est à dire le nombre d'images portant le même «patch» prédéfini.

$N_{ip} = \frac{N_{itot}}{N_p}$ où N_p est le nombre de «patchwork» que l'on peut produire. On a directement : $N_p = C_2^{p^2}$ d'où :

$$N_{ip} = \frac{2N^{p^2}}{p^2(p^2-1)} \tag{15.1}$$

Il est évident que plus la taille des patchs diminue par rapport à celle de l'image, plus le nombre d'images qui donnent une fausse alarme augmente.

15.2 Spread Spectrum

Nous avons vu paragraphe 2.1.1 les parallèles entre les méthodes à étalement de spectre et les méthodes de tatouage par patchwork. Lorsque l'on utilise l'étalement de spectre pour tatouer une image, il y a donc autant d'images allouées inconsidérément au propriétaire de la dite image que dans le cas d'une méthode par Patchwork.

Le fait d'utiliser une méthode d'insertion adaptative pour implémenter la marque ne change pas le problème puisque la procédure de détection reste identique.

15.3 Paquets d'ondelettes

Prenons pour K, la clef la plus précise, celle qui définit entièrement la meilleure base modifiée B^*. La détection de la marque dans une image quelconque I', est conditionnée par la distance de B^* à la meilleure base de I'. Autrement dit, toutes les images ayant pour meilleure base B^*, donnent une détection positive avec la clef K. On peut approximer le nombre moyen d'images possédant la même meilleure base par : $N_{ipo} = \frac{N_{itot}}{N_{bpo}}$ où N_{bpo} est le nombre de bases en paquets d'ondelettes. Chaque base en paquets d'ondelettes peut en effet être une meilleure base (il suffit par exemple de construire l'image en choisissant des coefficients sur la base qui respectent les contraintes énergétiques puis de reconstruire l'image). Si l'on appelle k_{apo} le niveau de décomposition de l'arbre de paquets d'ondelettes, N_{bpo} vérifie la relation de récurrence ci-dessous :

$$N_{bpo}(0) = 1 \tag{15.2}$$

$$N_{bpo}(k_{apo}+1) = N_{bpo}^4(k_{apo}) + 1 \tag{15.3}$$

On approxime cette suite par :

$$N_{bpo}(k_{apo}+1) = N_{bpo}(1)^{4^{k_{apo}}} \tag{15.4}$$

$$N_{bpo}(k_{apo}) = 2^{4^{k_{apo}-1}} \tag{15.5}$$

avec $k_{apo} = \frac{\log(p)}{\log(2)}$
d'où

$$N_{ipo} = \frac{N^{p^2}}{2^{4^{\frac{\log(p)}{\log(2)}-1}}} \tag{15.6}$$

ainsi

$$N_{ipo} = \frac{N^{p^2}}{2^{\frac{p^2}{4}}} \tag{15.7}$$

Si l'on prend par exemple $p = 4$, on a seulement 16 bases possibles permettant de représenter 3.10^{38} images.

Remarque : On a traité ici le pire des cas, on vu en effet au paragraphe 5.2.1 que le nombre de bases possibles respecte l'inéquation :

$$2^{2^{j-1}} \leq N_B \leq 2^{\frac{5}{4}2^{j-1}} \tag{15.8}$$

15.4 Comparaison

Nous comparons le nombre de fausses alarmes obtenus pour la méthode de Patchwork et la méthode en paquets d'ondelettes. L'équation suivante présente le rapport du nombre de ces fausses alarmes pour les deux méthodes :

$$\frac{N_{ip}}{N_{ipo}} = \frac{2^{1+\frac{p^2}{4}}}{p^2(p^2-1)} \tag{15.9}$$

Ce produit est très grand à partir de petites valeurs de p ($p > 10$) et tend rapidement vers l'infini. Pour $p = 256$, le rapport $Nip/Nipo$ vaut environ $\exp(4923)$. Notre méthode est donc moins sujette au fausses alarmes que le patchwork et l'étalement de spectre.

15.5 Conclusion

Dans ce paragraphe, nous avons calculé le nombre de fausses alarmes existantes pour une marque donnée et pour l'ensemble des images. Le fait que ces alarmes existent apporte un doute quand à l'utilisation même du tatouage pour la protection du copyright. En effet, dès qu'un propriétaire possède une marque, cette marque n'est pas implantée sur la seule image tatouée mais sur tout un ensemble d'images. Cependant il y a tant d'images dans la nature, qu'il y a peu de chance de tomber sur une image qui porte la marque à l'état original. De plus, il y a peu de chance que cette image soit intéressante d'un point de vue psychovisuel.

On a regardé ici le nombre d'image portant exactement la même marque. Il est évident que ce nombre augmente si l'on admet que la watermarque puisse être dégradée.

Nous avons aussi considéré que toutes les bases étaient équiprobables, ce qui n'est pas le cas avec des images réelles où l'énergie est par exemple plus présente dans les basses fréquences.

Sixième partie

Résultats

Chapitre 16

Résultats

16.1 Présentation des résultats

Nous avons appliqué notre méthode de tatouage sur les images de l'ensemble test présenté à la figure 16.1. Les noms de ces images sont respectivement : Lenna, Barbara, Bateau, Singe, Oiseau, Pont, Caméra, Fruits, Tableau et Poivron. Elles sont toutes de tailles 256×256 codées sous 8 bits par pixels.

FIG. 16.1 – Ensemble d'images test

16.1.1 Paramètres du processus de tatouage et de détection de la marque

Paramètres d'implémentation de la marque

Nous tatouons les images pour les deux ensembles de valeurs des processus de tatouage rassemblés dans le tableau 16.1. Nous appellerons T_1 le tatouage correspondant aux premier choix, T_2 aux seconds. La marque choisie est une séquence pseudo-aléatoire de longueur 32 bits que nous insérons avec une forte redondance. Nous avons en effet constaté au chapitre 12 que ce choix permet une meilleure détection que l'emploi des m-séquences.

TAB. 16.1 – Paramètres d'implémentation de la marque

Tatouage	Coefficient de redondance	Seuil de sélection s	Force de tatouage ε
T_1	20	10^{-6}	s
T_2	80	10^{-7}	$4s$

Paramètres de détection de la marque

Nous avons fixé la probabilité de faux positifs à $P_{fa} = 0.02\%$. Pour chaque image, nous ferons la détection pour deux seuils de sélection de la meilleure base : le seuil utilisé pour l'implémentation de la marque (appelé Détecteur1) et le seuil issu de l'étude faite au chapitre 10 (appelé Détecteur2).

Pour chaque attaque, nous donnerons le résultat de la détection par la réponse du détecteur : «oui», si la marque est retrouvée, «non» sinon. Certaines attaques (JPEG, cropping) dégradent plus ou moins la qualité de l'image en fonction d'un paramètre, dans ce cas, nous donnerons le paramètre de l'attaque la plus dégradante à laquelle résiste notre tatouage (nous avons vérifié que toutes les attaques moins dégradantes donnent une détection positive).

16.1.2 Choix des attaques

Les attaques utilisées sont les transformations présentes dans le logiciel Stirmark et présentées au chapitre 8.

Lorsque la taille des images test est modifiée par une attaque, on utilise le prétraitement déjà utilisé au chapitre 8 : on procède par cropping pour les images de trop grandes tailles et par miroir pour celles de trop petites tailles.

16.2 Résultats

16.2.1 Invisibilité

La mesure du PSNR obtenue pour les images tatouées est donnée dans le tableau 16.2. Ces valeurs sont toutes au dessus de 35 dB. La meilleure base de l'image fruit sélectionnée par le deuxième seuil s ne possède pas une structure permettant d'insérer une marque de redondance 80. Nous n'utiliserons que le premier tatouage pour cette image.

Les qualités visuelles des images fluctuent en fonctions des images tatouées. Comme on utilise des petits seuils de sélection de meilleures bases, les paquets sélectionnés ont une faible résolution spatiale ce qui entraîne des artefacts sur les zones les moins texturées. L'image bateau présentée à la figure 16.2 présente par exemple des déformations visibles sur le ciel. L'image singe, très texturée est de très bonne qualité après tatouage (voir la figure 16.3). Ces artefacts peuvent cependant disparaître si l'on diminue le paramètre de redondance ou la force du tatouage. On peut aussi faire subir un post-traitement

TAB. 16.2 – Mesure du PSNR pour chaque image tatouée (dB)

Image	Tatouage T_1	Tatouage T_2
Lenna	39.44	38.12
Bateau	37.44	35.8
Barbara	41, 14	39.36
Singe	42	38.57
Pont	40.27	38.62
Caméra	41.77	38.52
Fruits	37.63	
Tableau	38.95	36.75

à l'image tatouée visant à diminuer les modifications aux endroits où le tatouage est trop visible (voir le chapitre 11). Ces modifications du tatouage ont pour désavantage de diminuer la robustesse de la détection de la marque.

FIG. 16.2 – Image Bateau originale et image marquée

16.2.2 Robustesse à la compression JPEG

Le tableau 16.3 donne pour chaque tatouage et chaque image, la transformation JPEG de moins bonne qualité à laquelle résiste le tatouage. Par exemple le premier tatouage de l'image Lenna résiste à des compressions $JPEG$ allant de 100% à 50% de qualité pour le premier détecteur. On améliore ce résultat en utilisant le deuxième détecteur : la détection est alors possible après une compression de coefficient de qualité 40%. Pour toutes les images, les deux tatouages sont robustes à des compressions JPEG de coefficients de qualité supérieurs à 50%. Pour certaines images la détection est encore possible pour des

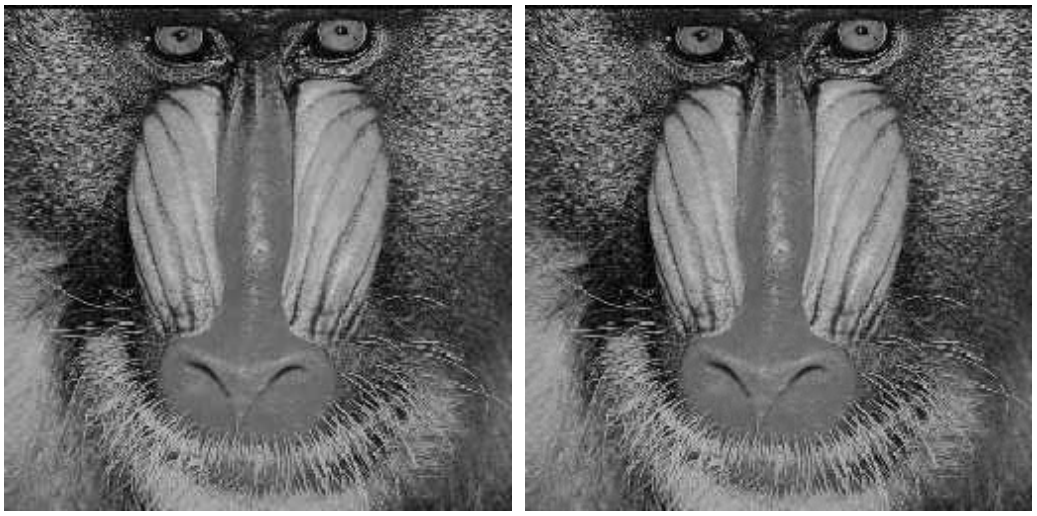


FIG. 16.3 – Image Singe originale et image marquée

TAB. 16.3 – Robustesse à la transformation JPEG (% de qualité)

	Tatouage1		Tatouage2	
	Détecteur1	Détecteur2	Détecteur1	Détecteur2
Lenna	50	40	30	35
Bateau	25	25	20	20
Barbara	30	40	20	20
Singe	50	50	30	30
Pont	35	35	30	30
Caméra	40	50	25	25
Fruits	25	25		
Tableau	40	30	20	20

coefficients de qualité inférieure (20% pour les images bateau et tableau tatoués avec le deuxième tatouage). La figure 16.4 présente l'image Lenna tatouée obtenue après une compression JPEG de 50% de qualité, des effets de blocs commencent à apparaître. La figure 16.5 présente l'image tableau tatouée après compression JPEG de 20% de qualité. Les artefacts apparaissent nettement.

Pour cette attaque, le deuxième tatouage donne de meilleurs résultats que le premier.

16.2.3 Robustesse au cropping

Le tableau 16.4 présente pour chaque image la transformation au cropping la plus forte à laquelle le tatouage a résisté. Par exemple, le tatouage1 de l'image lenna résiste à des cropping dont la taille varie de 1% à 25% de la taille de l'image. Nous obtenons de bons résultats puisque pour toutes les images, le tatouage résiste à des cropping allant

FIG. 16.4 – Image Lenna marquée avant et après une compression JPEG de coefficient de qualité de 20%, images et détails

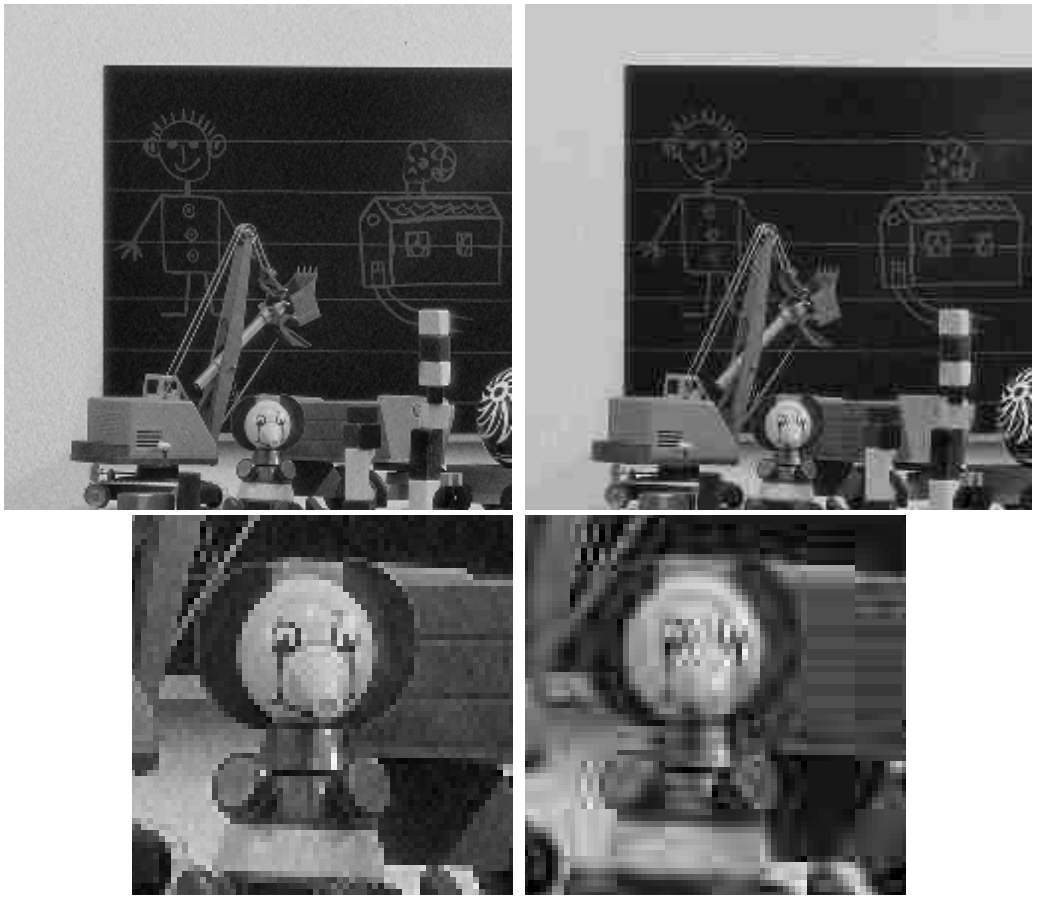


FIG. 16.5 – Image tableau marquée avant et après une compression JPEG de coefficient de qualité de 20%, images et détails

TAB. 16.4 – Robustesse au cropping (% de la taille de l'image)

	Tatouage1		Tatouage2	
	Détecteur1	Détecteur2	Détecteur1	Détecteur2
Lenna	25	15	15	15
Bateau	25	20	20	20
Barbara	15	5	10	10
Singe	10	5	15	
Pont	20	10	10	10
Camera	25	20	10	10
Fruits	20	25		
Tableau	25	15	15	15

de 1% à 10% de la taille l'image. La figure 16.6 présente l'image bateau avant et après cropping.

FIG. 16.6 – Image bateau marquée avant et après le cropping de 25% de la taille de l'image

16.2.4 Robustesse aux transformations géométriques

Le processus de tatouage par paquets d'ondelettes est particulièrement sensible aux transformations géométriques. En effet, du fait des décimations successives de l'image, la décomposition en ondelettes n'est pas invariante à la translation. La structure de la meilleure base n'est donc pas invariante aux transformations de ce type. C'est pourquoi, le tatouage proposé n'est pas robuste aux transformations de désynchronisation.

Notre méthode de tatouage est basée sur le choix d'une meilleure base représentant le comportement spatial et fréquentiel de l'énergie. Il est évident que si une attaque modifie ce comportement la détection sera fausse.

Translations

Enlever plusieurs lignes ou colonnes présente une attaque très dangereuse pour notre méthode. En effet, la meilleure base est alors modifiée, quelque soit le choix du seuil de sélection. Ces attaques sont donc concluantes et trompent notre détecteur.

Rotations

Deux types de rotations ont été étudiées : les rotations suivies d'un cropping de l'image et les rotations suivies d'un changement d'échelle. La décomposition en paquets d'ondelettes analysant l'image selon différentes orientations fréquentielles, il est claire que notre méthode est fragile à ces transformations.

Pour de très petites rotations, le détecteur permet cependant de retrouver la marque pour certaines images. Le tableau 16.5 rassemble les résultats obtenus. Nous pouvons conclure que pour cette attaque, notre algorithme n'est pas assez performant.

FIG. 16.7 – Image caméra tatouée avant et après une rotation de 0.5 degré

Changements d'échelles

Le processus de tatouage n'est pas robuste aux changements d'échelles.

Étirements

La méthode de tatouage est robuste aux étirements de 1% dans les deux directions sauf pour les images Ponts et Singe, dont le tatouage est fragile à un étirement selon les horizontales. Le tatouage T_2 de l'image Lenna est robuste à un étirement de 5% selon l'horizontal et celui de l'image fruit est robuste à un étirement de 5% selon la verticale.

TAB. 16.5 – Robustesse aux petites rotations avec changements d'échelles (en degré)

Image	rotation 0.25	rotation -0.25	rotation 0.5	rotation -0.5
Lenna (T_1,D_1)	non	non	non	non
Lenna (T_1,D_2)	oui	oui	non	non
Lenna (T_2,D_1)	non	non	non	non
Lenna (T_2,D_2)	oui	oui	non	non
Bateau (T_1,D_1)	oui	oui	non	oui
Bateau (T_1,D_2)	oui	oui	non	non
Bateau (T_2,D_2)	non	non	non	non
Bateau (T_1,D_2)	non	non	non	non
Barbara (T_1,D_1)	oui	non	non	non
Barbara(T_1,D_2)	non	non	non	non
Barbara (T_2,D_1)	oui	non	non	non
Barbara (T_2,D_2)	oui	non	non	non
Singe(T_1, D_1)	oui	non	non	non
Singe(T_1, D_2)	oui	non	non	non
Singe(T_2, D_1)	non	non	non	non
Singe(T_2, D_2)	non	non	non	non
Pont (T_1,D_1)	non	non	non	non
Pont (T_1,D_2)	non	oui	non	non
Pont (T_2,D_1)	non	non	non	non
Pont (T_2,D_2)	oui	non	non	non
Camera (T_1,D_1)	oui	oui	non	non
Camera (T_1,D_1)	oui	oui	non	oui
Camera (T_2,D_1)	oui	non	non	non
Camera (T_2,D_2)	oui	non	non	non
Fruits (T_1,D_2)	oui	non	non	non
Fruits (T_1,D_2)	oui	oui	non	non
Tableau (T_1,D_1)	non	non	non	non
Tableau (T_1,D_2)	oui	non	non	non
Tableau (T_1,D_2)	oui	oui	non	non
Tableau (T_1,D_2)	oui	non	non	non

Transformations linéaires

Le tatouage est fragile à ce type de transformation.

Transformation Stirmark

Les détecteurs utilisés ne détectent plus le code après une transformation Stirmark. Pour détecter celle ci, il faut accroître la probabilité de faux positif. La détection est possible si l'on autorise un nombre de faux positifs d'environ 5%. Le meilleur résultat est obtenu pour l'image Lenna, pour le deuxième tatouage en utilisant le seuil optimisé à la détection et pour un nombre de faux Positif de 0.1%.

16.2.5 Robustesse aux filtrages

Le logiciel permet de tester trois sorte de filtrages : un filtrage gaussien, un filtrage passe haut et trois filtrages moyenneurs (de tailles (2×2), (3×3) et (4×4)). Pour ces transformations, le processus de tatouage T_1 donne de mauvais résultats sauf pour l'image fruits. Cependant, avec les paramètres choisis pour T_2, les résultats sont meilleurs : ils sont rassemblés dans le tableau 16.6. Pour le premier type de filtrage, nous notons dans le tableau 16.6 les différents filtres auxquels le tatouage résiste, pour les deux autres type de filtrage, nous notons la réponse du détecteur.

Comme les transformations sont assez visibles, nous estimons que les résultats obtenus sont satisfaisants. La figure 16.8 présente l'image Barbara obtenue après tatouage et pour les différents filtrages (respectivement les filtres moyenneurs (2×2), (3×3) et (4×4) puis le filtre gaussien et le passe-haut).

16.3 Conclusion

Nous avons présenté dans ce chapitre les résultats obtenus pour la méthode que nous proposons. Ces résultats montrent un excellent comportement de notre détecteur face à des compressions JPEG et un bon comportement face à des filtrages et des cropping. Cependant, le principal défaut de notre algorithme de tatouage est le manque de robustesse aux transformations géométriques. Ce manque de robustesse provient d'une instabilité de la meilleure base à la fois face à des translations et des rotations. En effet, du fait des décimations successives, la décomposition en ondelettes discrète est non invariante à la translation, la meilleure base est donc *a fortiori* instable. La non-invariance aux rotations provient de la décomposition du signal suivant les orientations horizontales, verticales et diagonales lors de l'application de l'algorithme pyramidal. Pour avoir une base invariante aux translations, une solution serait d'utiliser l'algorithme «à trou» généralisé aux paquets d'ondelettes, avec pour désavantage une très grande augmentation de la complexité de l'algorithme de tatouage. Pour rendre la méthode robuste aux rotations, une idée, que nous n'avons pas testé par manque de temps, consisterait à travailler avec une ondelette $2D$ non séparable, ne privilégiant aucune orientation lors de la décomposition du signal.

FIG. 16.8 – Image caméra tatouée avant et après filtrage (on utilise respectivement les filtres moyenneurs (2×2), (3×3) et (4×4) puis le filtre gaussien et le passe-haut)

TAB. 16.6 – Robustesse aux filtrages

Image	filtrage moyenneur	filtrage gaussien	passe haut
Lenna (T_2,D_1)	(3×3)	oui	oui
Lenna (T_2,D_2)	(3×3)	oui	non
Bateau(T_2,D_1)	(3×3),(2×2)	oui	oui
Bateau(T_2,D_2)	(3×3),(2×2)	oui	non
Barbara (T_2,D_1)	(3×3),(2×2)	oui	non
Barbara (T_2,D_2)	(3×3),(2×2)	oui	non
Singe (T_2,D_1)	aucun	oui	non
Singe (T_2,D_2)	aucun	oui	non
Pont (T_2,D_1)	aucun	oui	non
Pont (T_2,D_1)	aucun	oui	non
Caméra (T_2)	aucun	non	non
Fruits (T_1,D_1)	(3×3),(2×2)	oui	non
Fruits (T_1,D_2)	(3×3),(2×2),(4×4)	oui	oui
Tableau (T_2,D_1)	(3×3),(2×2)	oui	oui
Tableau (T_2,D_2)	(3×3),(2×2)	oui	oui

Septième partie

Conclusion

Conclusion

Nous avons introduit ce travail en présentant et en définissant les objectifs du tatouage d'images numériques. Nous avons insisté pour considérer une approche globale du problème, elle nous a conduit à choisir un domaine applicatif : la protection du copyright et à en établir le cahier des charges. Après avoir présenté quelques méthodes génériques, nous avons choisi de travailler sur les techniques d'implémentation de la marque dites virtuelles.

Nous avons alors présenté la méthode développée pendant cette thèse, elle consiste à représenter une image par une structure en meilleure base de paquets d'ondelettes. La marque sera implémentée en déformant cette structure. La suite de notre travail vise à analyser les comportements de notre méthode face à un grand ensemble d'attaques puis à trouver des stratégies visant à diminuer l'effet de ces attaques. Nous nous sommes en particulier attaché à rechercher le seuil optimum définissant la meilleure base à l'aide d'une approche stochastique. Enfin, afin de respecter le cahier des charges, nous avons mis en oeuvre une méthode permettant de certifier que le tatouage ne dégrade pas l'image marquée. La partie suivante de ce rapport permet d'analyser la méthode proposée. A ce propos, nous avons présentés diverses solutions à des attaques intentionnelles. Une méthode clef publique/clef privée dite par «leurres» a été mis en oeuvre.

La dernière partie de ce rapport présente les résultats que nous avons obtenus. Ces résultats sont très hétéroclites selon les attaques testées et montrent en particulier les problèmes dus à la non-invariance de la meilleure base aux transformations géométriques.

Les perspectives ouvertes par ce travail peuvent être résumées en trois points. Le premier porte sur la nécessité de se soustraire à la non-invariance à la translation de la méthode. Pour cela, on peut envisager d'utiliser des ondelettes non-séparables, dont l'utilisation n'induit pas d'orientation particulière. A l'inverse, choisir des ondelettes dérivant de filtres proches de ceux utilisés par les modèles du SVH, nous permettrait une meilleure approche du compromis invisibilité/robustesse. On peut aussi envisager de calculer directement le masque psychovisuel dans le domaine des paquets d'ondelettes.

Une autre extension de ce travail concerne le développement de la méthode à clef privée-publique. L'intérêt de cette méthode est que pour un même tatouage, la sécurité est à deux niveaux. Le premier permet de savoir si l'image a été attaquée et le second oblige le pirate a dégrader l'image pour accéder à la marque. Enfin, on peut envisager d'adapter la méthode de tatouage par paquets d'ondelettes à d'autres applications que la protection du copyright et à d'autres supports que les images fixes.

Bibliographie

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn. Information hiding – a survey. *Proceedings of the IEEE (USA)*, 87(7) :1062–1078, 1999.

[2] A. Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX :5–38, Janvier 1883.

[3] B. Chen and G. Wornell. An information–theoretic approach to the design of robust digital watermarking systems. In *International Conference on Acoustic, Speech and Signal Processing (ICASSP)*, Phoenix, AZ, March 1999.

[4] S. Craver, N. Memon, B.L. Yeo, and M.M. Yeung. Can invisible watermarks resolve rightful ownerships ? Technical report, IBM, 1996.

[5] M. Kutter and F.A.P. Petitcolas. A fair benchmark for image watermarking systems. *Electronic Imaging : Security and Watermarking of multimedia Contents*, 3657 :226–239, January 1999.

[6] CCIR. Projet de révision de la recommandation 500-4 : Méthode d'évaluation subjective de la qualité des images de télévision. *Document commissions d'études du CCIR*, 11/BL/51-F, 1992.

[7] N. Bekkat. *Critère objectif de Qualité Subjective d'Images Monochromes. Conception du Modèle et Validation Expérimentales.* Thèse de doctorat d'état, IRESTE-laboratoire SEI, Nantes, France, Decembre 1999.

[8] S. Daly. The visible difference predictor : An algorithm for the assessment of image fidelity. In SPIE, editor, *Human vision, visual processing and digital display III*, volume 1666, pages 2–15, San-Jose (CA, USA), January 1992.

[9] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12) :1673–1687, 1997.

[10] Unsign. Unsign. *http ://www.altern.org/watermark.*

[11] S. Karzenbeisser and F.A.P. Petitcolas. *Information hiding techniques for steganography and digital watermarking.* Artech House, 1999.

[12] Digimarc. Digimarc. *http ://www.digimarc.com.*

[13] F. Hartung and M. Kutter. Multimedia watermarking techniques. *Proceedings of the IEEE*, 87(7) :1079–1107, jul 1999.

[14] A.M. Alattar. Smart images using digimarc's watermarking technology. In SPIE, editor, *Security and Watermarking of multimedia contents*, volume 3971, pages 246–263, San-Jose (CA, USA), January 2000.

[15] K. Tanaka, Y. Nakamura, and K. Matsui. Embedding secret information into dithered multilevel image. In *Proc. 1990 IEEE Military Commununication Conference*, pages 216–220, september 1990.

[16] G. Caronni. Assuring ownership rights for digital images. In H. H. Brueggemann and W. Gerhardt-Haeckl, editors, *Proceedings of Reliable IT Systems VIS '95*, Germany, 1995. Vieweg Publishing Company.

[17] C.F. Osborne, A.Z. Tirkel, G.A. Rankin, R. van Schyndel, W.J. Ho, and N. and Mee. Electronic water mark. In *Digital Image Computing, Technology and Applications*, pages 666–672, Sydney Australia, 1993.

[18] R. Van Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark. In *1st IEEE International Conference on Image Processing*, volume II, pages 86–90, Austin Texas USA, 1994.

[19] P. Bas. *Méthodes de tatouage d'images fondées sur le contenu*. PhD thesis, Institut National Polytechnique de Grenoble, Octobre 2000.

[20] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35(3&4) :313–336, 1996.

[21] I. Pitas and T. H. Kaskalis. Applying signatures on digital images. In *IEEE Workshop on Nonlinear Image and Signal Processing*, pages 460–463, Neos Marmaras, Greece, June 1995.

[22] G.C. Langelaar, J.C.A. van der Lubbe, and J. Biemond. Copy protection for multimedia data based on labeling techniques. In *Proceedings of the 17th Symposium on Information Theory in the Benelux*, pages 33–39, Enschede, The Netherlands, 1996.

[23] B. Macq and I. Pitas. Editorial of special issue on watermarking. *Signal Processing*, 66(3) :281–282, may 1998.

[24] J.F. Delaigle, C De Vleeshouwer, and B. Macq. A psychovisual approach for digital picture watermarking. *Journal of Electronic Imaging*, 7(3) :628–640, July 1998.

[25] J.F. Delaigle, C De Vleeshouwer, and B. Macq. Watermaking algorithm based on a human visual model. *Signal Processing*, 66 :319–336, May 1998.

[26] V. Darmstaedter, J.F. Delaigle, J.J. Quisquater, and B. Macq. Low-cost spatial watermarking. *Computer and Graphics*, 22 :417–424, 1998.

[27] B. Macq and J.L. Dugelay. Technologies du tatouage pour l'authentification et la protection des images. *Annales des Télécommunications*, 55(3-4) :99–100, 2000.

[28] E. Koch and J. Zhao. Towards robust and hidden image copyright labeling. In *Proc. of 1995 IEEE Workshop on Nonlinear Signal and Image Processing*, pages 452–455, Halkidiki, Greece, June 1995.

[29] J. Ó Ruanaidh. Watermarking digital images for copyright protection. In *Electronic Imaging and the Visual Arts*, Florence, Italy, February 1996.

[30] J. Ó Ruanaidh and T. Pun. Rotation, translation and scale invariant digital image watermarking. In *IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97)*, Santa Barbara, California, October 1997.

[31] L. Boney, A. H. Tewfik, and K. N. Hamdy. Digital watermarks for audio signals. In *1996 IEEE Int. Conf. on Multimedia Computing and Systems*, pages 473–480, Hiroshima, Japan, 1996.

[32] JPEG. The joint photographic experts group. *http ://www.jpeg.org*.

[33] G. R. Arce and L. Xie. A blind digital image signature in wavelet compression. In *IEEE Trans. Signal Processing*, volume IL, Chicago, Oct. 1998.

[34] D. Kundur and D. Hatzinakos. A robust digital image watermarking scheme using the wavelet-based fusion. In *IEEE Signal Processing Society 1997 International Conference on Image Processing (ICIP'97)*, Santa Barbara, California, October 1997.

[35] P. Loo and N. G. Kingsbury. Digital watermarking using complex wavelets. In *Proc. IEEE Conf. on Image Processing*, Vancouver, September 2000.

[36] M. Barni, F. Bartolini, A. Cappellini, V. Lippi, and A. Piva. A dwt-based algorithm for spatio-frequency masking of digital signatures. In *Proceedings of SPIE*, volume 3657, San Jose, CA, January 1999.

[37] F. Autrusseau, A. Saadane, and D. Barba. Psychovisual approach for watermarking. *SPIE Electronic Imaging*, January 2001.

[38] T. Kalker, G. Depovere, J. Haitsma, and M. Maes. A video watermarking system for broadcast monitoring. In *Proc. SPIE*, pages 103–112, January 1999.

[39] S. Winkler and M. Kutter. Vers un tatouage à étalement de spectre opimal utilisant le système visuel humain. In *Coresa'99*, Institut-Eurocom, Sophia Antipolis, France, June 1999.

[40] J.-F. Delaigle, J.-M. Boucqueau, J.-J. Quisquater, and B. Macq. Digital images protection techniques in a broadcast framework : An overview. TALISMAN project report, ACTS project AC019, Université Catholique de Louvain Laboratoire de télécommunications et télédétection, Brussels, Belgium, 1996.

[41] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. In *Proceedings of SPIE Photonics East'96 Symposium*, Boston, Massachusetts, 1996.

[42] B. Chen and G. Wornell. An information–theoretic approach to the design of robust digital watermarking systems. In *International Conference on Acoustic, Speech and Signal Processing (ICASSP)*, Phoenix, AZ, March 1999.

[43] D. Kundur and D. Hatzinakos. Digital watermarking using multiresolution wavelet decomposition. In *International Conference on Acoustic, Speech and Signal Processing (ICASSP)*, volume 5, pages 2969–2972, Seattle, Washington, U.S.A., may 1998. IEEE.

[44] E. Hitti. *Sélection d'un banc optimal de filtres à partir d'une décomposition en paquets d'ondelettes. Application à la détection de saut de fréquences dans des signaux multicomposantes.* PhD thesis, Université de Nantes, 1999.

[45] S. Mallat. *A wavelet tour of signal processing.* Academic Press, 1998.

[46] P. Abry. *Transformée en ondelettes, analyse multirésolution et signaux de pression en turbulence.* PhD thesis, Université C. Bernard Lyon I, 1994.

[47] Y.T. Chan. *Wavelet basics.* Kluwer Academic Publisher, 1995.

[48] G. Strang. *Wavelet and filter bank.* Wellesley Cambridge Press, 1996.

[49] M. Vetterli. Wavelet and filter banks : Theory and design. *IEEE trans. on signal processing*, 41(8) :2207–2232, 1990.

[50] M.V. Wickerhauser. Lectures on wavelet packet algorithms. *INRIA*, pages 31–99, 1991.

[51] M.V. Wickerhauser R.R. Coifman. Entropy based algorithms for best basis selection. *IEEE transaction on Information Theory*, 38(2) :713–778, 1992.

[52] R. Coifman, Y. Meyer, S. Quake, and M. V. Wickerhauser. Signal processing and compression with wave packets. Technical report, Yale University, 1990.

[53] D. L. Donoho and I. M. Johnstone. Ideal denoising in an orthonormal basis chosen from a library of bases. Technical report, 1994.

[54] N. Saito and R. R. Coifman. Local discriminant bases. In A. F. Laine and M. A. Unser, editors, *Wavelet Applications in Signal and Image Processing II, Proc. SPIE 2303*, pages 2–14, 1994.

[55] A. Sostaric, D. Zazula, and C. Doncarli. Feature extraction using wavelet packets. *Elektroteshniska in racuanalniska konferenca*, 4 :645–648, 1996.

[56] A. Manoury, J. Lévy-Véhel, and M.F. Lucas. Watermarking d'images par paquets d'ondelettes. In *17^e colloque GRETSI sur le Traitement du Signal et des Images*, volume 2, pages 275–278, Vannes, France, 13-17 septembre 1999.

[57] J. Lévy-Véhel and A. Manoury. Wavelet packets based digital watermarking. In *17^e International Conference on Pattern Recognition*, volume 3, pages 417–421, Barcelona, Spain, 3-8 septembre 2000.

[58] C. Fontaine. *Contribution à la recherche de fonctions booléennes hautement non linéaire, et au marquage d'images en vue de la protection des droits d'auteur.* PhD thesis, Université de paris 6, 1998.

[59] R.J. McEliece. *Finite fields for computer scientist and engineers.* Kluwer Academic Publishers, 1998.